ON ELLIPTIC CURVE CRYPTOSYSTEMS

A Thesis Submitted

in Partial Fulfilment of the Requirements

for the Degree of

MASTER OF TECHNOLOGY

by

KALYAN KUPPUSWAMY

to the

DEPARTMENT OF ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY

February 1994

Certificate

It is certified that the work contained in the thesis entitled **"On Elliptic Curve Cryptosystems"** has been carried out by Kalyan Kuppuswamy under my supervision and that this work has not been submitted elsewhere for a degree.

2-2-94

M. U. Siddiqi
Professor
Department of Electrical Engineering
I. I. T. Kanpur

February 1994.

Abstract

The traditional Cryptographic schemes used for Public-Key Systems like Pohlig-Hellman, El Gamal, Massey-Omura, etc. based on finite fields are being seriously threatened due to recent advances in solving the discrete logarithm problem over finite fields. Also newer and faster methods of factoring integers (upto 100 digits) have made schemes like Rivest, Shamir and Adleman (RSA), based on finite rings, vulnerable to such attacks. Against this background, efforts are on to base the existing cryptographic schemes over more general structures, notably the elliptic curve groups and matrix ring groups, over which such attacks may become inoperative. In this thesis, we look into the theory aspects of the elliptic curve algebra, try to adapt the existing Public-Key cryptographic schemes like Pohlig-Hellman, etc. on elliptic curve groups and more importantly from the practical viewpoint, discuss the various key implementation aspects like computational complexity, faster encryption, etc. that arise with these modified cryptosystems. Also a new generalisation, *i.e* cryptosystems based over monoids is carried out for elliptic curves based over finite rings which is the elliptic curve equivalent of the RSA scheme. The entire discussion is written in a Tutorial format and examples *(simulated using C language source code)* have been profusely quoted to illustrate the theory aspects.

TO MY PARENTS

Acknowledgements

I express my deepest gratitude to Prof. M.U.Siddiqi for having given me valuable suggestions and the freedom to work on the topic. Also my sincere thanks to Balvinder for helping out in various stages of the work and to Ashish, Venkatesh, Anjani and Abhay for memorable moments in the IP Lab And to S.P, Shailesh, Goyaljee and others for their wonderful company during my stay at IIT Kanpur

Kalyan Kuppuswamy

Table Of Contents

Chapter 1 : Introduction

Chapter 2 : Review of Cryptology

Chapter 3 : Elliptic Curve Structures over Finite Fields

List of Figures and Tables

Chapter 1
Introduction

1.1 General Nature of the Problem

For thousands of years, *Cryptography* has been the art of providing secure communication over insecure channels, and *Cryptanalysis* has been the dual art of breaking into such communications. Historically, this combined art called *Cryptology* has been almost exclusively in the hands of military and diplomats. However, with the advent of the computer revolution, and a society where vast amounts of personal, financial, commercial and technological information are stored in computer data banks and transferred over computer networks, the necessity for civilian cryptography has become overwhelming.

With the advances in science and technology, the age-old battle between cryptography and cryptanalysis has taken a new dimension. The enormous increase in computing power and the advent of parallel processing has placed the cryptanalyst in a far more favourable position and many of the existing cryptosystems have been completely broken or seriously threatened. And cryptologists are working towards finding objective criteria for the security of the cryptosystems, thereby transforming this ancient art into an exact science

1.2 Motivation and Scope of the Work

The problems in the area of cryptography which draw our attention are

a) How do the present cryptographic systems stand upto cryptanalytic attacks?

b) If not, can we look for new cryptographic systems which could possibly withstand these attacks ?

c) The underlying theory behind the new cryptosystem design.

d) The engineering aspects like computation complexity etc. involved.

In this thesis, we shall tackle some of the above problems. In cryptographic literature, there exist two schemes of encryption - private-key and public-key systems. We shall restrict our attention to public key systems only.

We can divide the existing cryptographic schemes on public-key systems into two categories

1) Cryptosystems based on finite field structure like Diffie-Hellman, Pohlig-Hellman, Massey-Omura schemes [5, 10, 15].

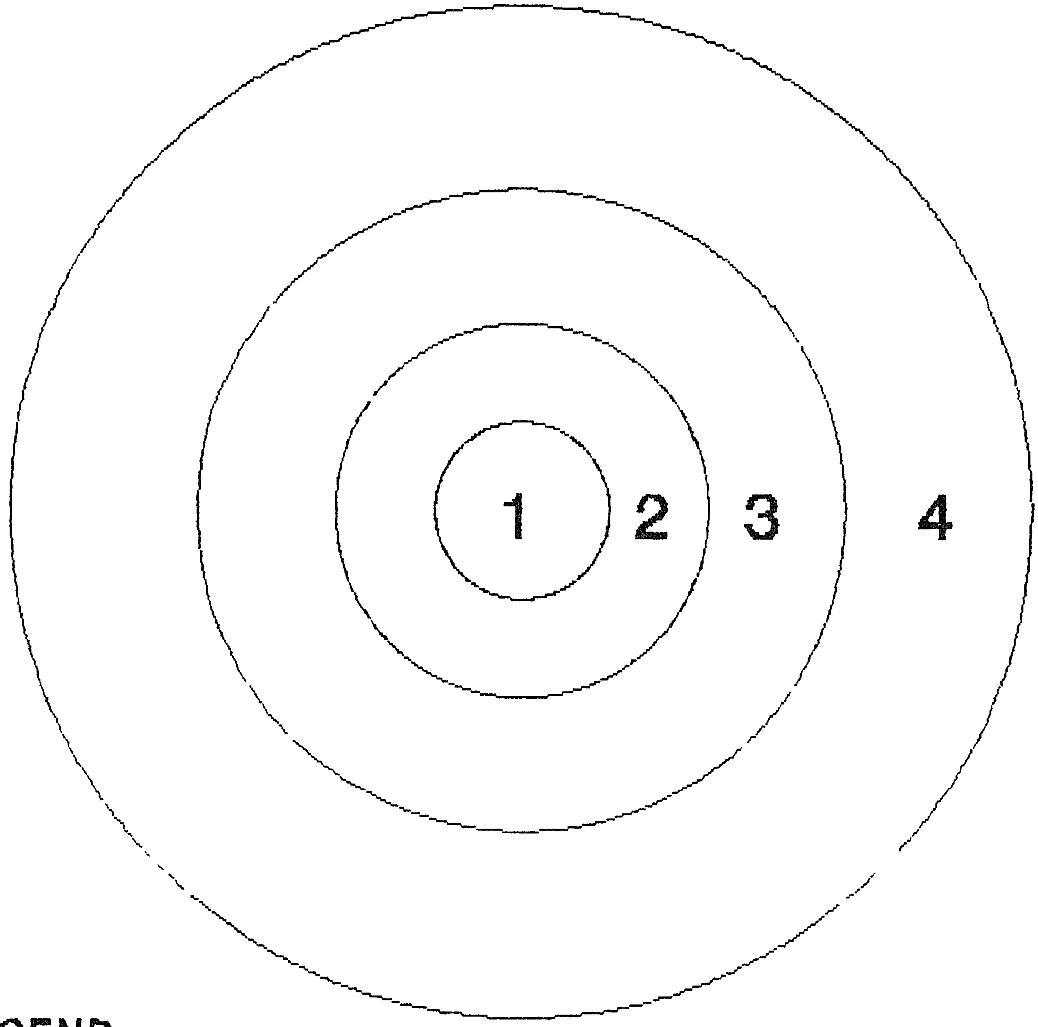
2) Cryptosystems based on finite ring structure like Rivest, Shamir and Adleman (RSA) scheme [5, 10, 15].

However, improved methods in solving the discrete logarithm problem [2, 4, 5, 11, 19] over finite groups and factorization [2, 4, 5, 21] techniques have threatened these existing methods. There could be two approaches to ward off the threat. One, simply search for higher and higher order of groups which are beyond the computational reach of modern day computers (orders like 200 digit primes) and wait till improved technology catches up with it and increase the order then and so on. But this *hide and seek* approach is a rather simplistic solution and an altogether different approach to the problem is required. A second method could be as following. If one looks carefully into the nature of these attacks, one finds that it is the *multiplicative* structure offered by fields and rings, over which cryptosystems are designed, that are being exploited for cryptanalytic attacks. Hence, a cryptosystem defined over a *lesser* restrictive structures, † it is reasonable to assume at an intuitive level that most of the cryptanalytic attacks can be avoided. A general picture of our method of classification is depicted in Figure 1. We shall substantiate upon our general observation in the text later.

The elliptic curve algebra defined over fields and rings promises us this requisite structure. We shall look deeper into the theory aspects of this algebra, try to adapt the existing public-key cryptographic schemes like Pohlig-Hellman,etc. on elliptic curve groups and more importantly from the practical viewpoint, look into various implementation aspects that arise with these modificated cryptosystems.

† *by that we mean structures with only one operation defined, addition, like groups or monoids, unlike structures like fields or rings over which we have two operations, addition and multiplication*

FIG. 1: CLASSIFICATION OF CRYPTOGRAPHIC SYSTEMS



LEGEND

1: CRYPTOGRAPHIC SYSTEMS OVER FIELDS

2: CRYPTOGRAPHIC SYSTEMS OVER RINGS

3: CRYPTOGRAPHIC SYSTEMS OVER GROUPS

4: CRYPTOGRAPHIC SYSTEMS OVER MONOIDS

1.3 Organisation of the Work

Chapter 2 gives the review of the existing public-key cryptosystems and a summary of the recent advances in breaking some of the ciphers.

Chapter 3 gives the necessary algebraic background required to understand elliptic curve cryptosystems. We also narrow down on certain classes of elliptic curves for implementation purposes and discuss procedures for embedding message texts for encryption.

In Chapter 4, we discuss the elliptic curve analogs of the existing public-key cryptosystems, how they offer better security against traditional cryptanalytic attacks. Also a new generalisation of the existing cryptosystems is presented. Choice of elliptic curves for preventing cryptanalytic attacks are discussed.

Chapter 5 gives the engineering aspects involved in implementation of elliptic curve public-key cryptosystems *viz.* efficient encryption, choice of basis functions, for faster encryption etc.

In Chapter 6, we conclude with a comparison with the existing public-key systems and discuss the scope for future work in this area.

Chapter 2
Review of Cryptology

We start with a few basic definitions in the area of Cryptology.

2.1 Cryptological Concepts

Cryptography is the science and study of secret writing. A cipher is a secret method of writing, whereby *plaintext (or cleartext)* is transformed into *ciphertext (also called cryptogram)*. The process of transforming plaintext into ciphertext is called encipherment or *encryption*; the reverse process of transforming ciphertext into plaintext is called decipherment or *decryption*. Both encipherment and decipherment are controlled by a cryptographic key.

Cryptanalysis is the science and study of methods of breaking ciphers. A cipher is breakable if it is possible to determine the plaintext or key from the ciphertext, or to determine the key from plaintext-ciphertext pairs.

The branch of knowledge embodying both cryptography and cryptanalyis is called *Cryptology* [5, 10, 15].

2.2 Cryptographic System

A cryptographic system (or cryptosystem) has five components [10]

1. A plaintext message space M

2. A ciphertext message space C

3 A key space κ

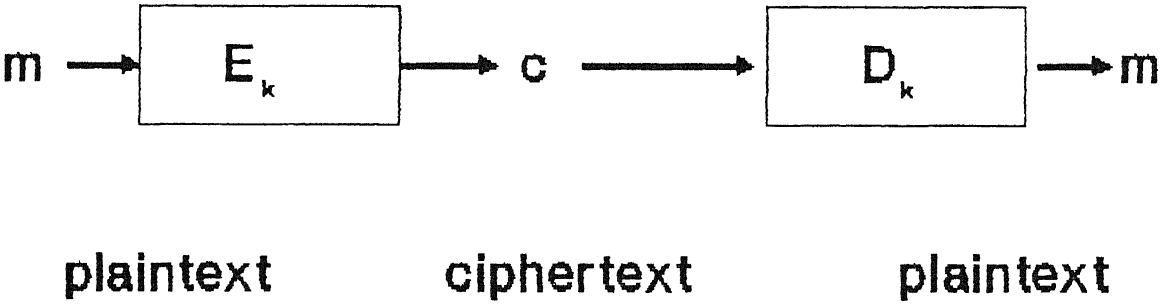
4. A family of enciphering transformations

$$E_k : M \rightarrow C, \text{ where } k \in \kappa \qquad (2.2.1)$$

5. A family of deciphering transformations

$$D_k : C \rightarrow M, \text{ where } k \in \kappa \qquad (2.2.2)$$

FIG. 2: CRYPTOGRAPHIC SYSTEM



A general picture of a cryptographic system is depicted in Figure 2.

Cryptosystems must satisfy three general requirements

1. The enciphering and deciphering transformations must be efficient for all keys.
2. The system must be easy to use.
3. The security of the system should depend only on the secrecy of the keys and not on the secrecy of the algorithms E and D.

There are specific requirements for secrecy and authenticity [10]. Secrecy requires that a cryptanalyst not be be able to determine plaintext data from intercepted ciphertext. Formally, there are two requirements

a) It should be computationally infeasible for a cryptanalyst to systematically determine the deciphering transformations D_k from intercepted ciphertext c, even if the corresponding plaintext m is known.

b) It should be computationally infeasible for a cryptanalyst to systematically determine plaintext m from intercepted ciphertext c.

Data authenticity requires that a cryptanalyst not be able to substitute a false ciphertext c' for a ciphertext c without detection. Formally, the two requirements are

a) It should be computationally infeasible for a cryptanalyst to systematically determine the enciphering transformations E_k from intercepted ciphertext c, even if the corresponding plaintext m is known.

b) It should be computationally infeasible for a cryptanalyst to systematically find ciphertext c' such that $D_k(c')$ is a valid plaintext in the set.

Cryptosystems can be classified in two categories [5, 10, 15]

i) Secret-key or private cryptosystem

ii) Public-key or public cryptosystem.

A general cryptosystem is secret-key if some secret piece of information (*the key*) has to be agreed ahead of time between any two parties that wish to communicate through the cryptosystem

This need of secure key distribution was not a major problem in the days when cryptography was for the few. Now that cryptography has gone public, it is unreasonable to set up a network in which each pair of potential users share a secret key in advance, because the number of keys would grow quadratically with the number of users.

To overcome this difficulty and ensure secure communication over insecure channels between two totally unacquaninted parties, the concept of public-key cryptosystem was evolved.

2.3 Public-Key Cryptosystems

The concept of two-key cryptosystem was introduced by Diffie and Hellman in 1976. They proposed a new method of encryption called Public-key encryption [5, 10, 15], wherein each user has both a public and private key, and two users can communicate knowing only each other's public keys.

In a public-key system, each user A has a public enciphering transformation E_A, which may be registered with a public directory, and a private deciphering transformation D_A, which is known only to that user. The private transformation D_A is described by a private key, and the public transformation by the public key derived from the private key by the one-way transformation. It must be computationally infeasible to determine D_A from E_A.

In a public-key system, secrecy and authenticity are provided by the seperate transformations. Suppose user A wishes to send message m to another user B. If A knows $B's$ public transformation E_B, A can transmit m to B in secrecy by sending the ciphertext $c = E_B(m)$. On receipt, B deciphers c using $B's$ private transformation D_B, getting

$$D_B(c) = D_B(E_B(m)) = m \tag{2.3.1}$$

The preceding scheme does not offer authenticity because any user with access to $B's$ public transformation could substitute another message m' for m by replacing c with $c' = E_B(m')$.

For authenticity, m must be transformed by $A's$ own private transformation D_A. Ignoring secrecy for the moment, A sends $c = D_A(m)$ to B. On receipt, B uses $A's$ public transformation E_A to compute

$$E_A(c) = E_A(D_A(m)) = m \tag{2.3.2}$$

Authenticity is provided because only A can apply the transformation D_A. Secrecy is not provided because any user with access to $A's$ public transformation can recover m.

To achieve both secrecy and authenticity, the sender and receiver must each apply two sets of transformation. Suppose A wishes to send a message m to B. First $A's$ private transformation D_A is applied. Then A enciphers the result using $B's$ public encryption transformation E_B, and transmits the doubly transformed message $c = E_B(D_A(m))$ to B. B recovers m by first applying $B's$ own private deciphering transformation D_B, and then applying $A's$ public transformation E_A to validate its authenticity, getting

$$\begin{aligned} E_A(D_B(m)) &= E_A(D_B(E_B(D_A(m)))) \\ &= E_A(D_A(m)) \\ &= m \end{aligned} \tag{2.3.3}$$

2.4 Public-Key Systems based on Exponentiation Ciphers

In this section, we shall discuss the major cryptographic schemes which emerged after Diffie and Hellman's pioneering breakthrough in cryptographic studies.

All these cryptosystems [5, 10, 15] are based on encryption based on computing exponentials over a finite field. The enciphering and deciphering transformations are based on Euler's generalisation of Fermat's Theorem.

First, let us discuss Euler's Totient Function [10, 18]

Definition: *Given an integer n, $\phi(n)$ is the number of elements in the reduced set of residues modulo n. $\phi(n)$ is the number of positive integers less than n that are relatively prime to n.*

In general, for an arbitrary n, $\phi(n)$ is given by

$$\phi(n) = \prod_{i=1}^{t} p_i^{e_i-1}(p_i - 1) \tag{2.4.1}$$

where

$$n = p_1^{e_1} p_2^{e_2} \cdot\cdot p_t^{e_t}$$

Theorem 2.4.1. *(Fermat's Little Theorem) [10, 18] Let p be prime. Then for every a such that $gcd(a, p) = 1$,*

$$a^{p-1} \equiv 1 \pmod{p} \tag{2.4.2}$$

Euler provided a generalised version of the above theorem.

Theorem 2.4.2. *(Euler's generalisation) [10, 18] For every a and n such that $gcd(a, n) = 1$,*

$$a^{\phi(n)} \equiv 1 \pmod{n} \tag{2.4.3}$$

Proof: Let $r_1, r_2, \cdots r_{\phi(n)}$ be the reduced set of residues modulo n such that $0 < r_i < n$ for $1 \leq i \leq \phi(n)$. Therefore,

$$\prod_{i=1}^{\phi(n)} (ar_i) \equiv \prod_{i=1}^{\phi(n)} (r_i) \pmod{n} \tag{2.4.4}$$

By cancellation,

$$a^{\phi(n)} \equiv 1 \pmod{p}$$

2.4.1 Pohlig-Hellman Scheme

In this scheme [5, 10, 15], enciphering a message block $m \in Z_n$ is done by computing the exponential

$$c \equiv m^e \pmod{p} \tag{2.4.5}$$

where p is a large prime $\in Z$ and $C \in Z_p$. Here e and p are the keys to the enciphering transformation.

m is restored by the same operation, but by using a different exponential d for the key

$$m \equiv c^d \pmod{p} \tag{2.4.6}$$

such that

$$ed \equiv 1 \pmod{\phi(p)} \tag{2 4 7.a}$$

Since p is prime,

$$\phi(p) = p - 1 \qquad (2.4.7.b)$$

The security of the scheme rests on the complexity of computing discrete logarithms in Z_p. This is because under a known plaintext attack, a cryptanalyst can compute e (and thereby d) given a pair (m, c)

$$c = log_m c \text{ in } Z_p \qquad (2.4.8)$$

Pohlig and Hellman [10] show that if $(p-1)$ has only small prime factors, it is possible to compute the logarithm in $O(logp)$ time, which is unsatisfactory even for large values of p. The fastest known algorithm for computing the discrete logarithm in Z_p, due to Adleman takes approximately

$$T = exp(sqrt(lnp(lnln(p))) \text{ steps} \qquad (2.4.9)$$

Consider an example, if p is 200 bits long, then Equation (2.4.9) evaluates to $T = 2.7 \times 10^{11}$. Assuming 10^{11} steps can be performed per day (i.e. about 1 step per microsecond), the entire computation would take only a few days.

Pohlig and Hellman also note that their scheme could be implemented in the Galois Field F_{2^n}, where $2^n - 1$ is a large prime number called Mersenne prime [18]. Such an implementation would be efficient and have the advantage that all messages would require exactly n bits; furthermore, every element in the range $(1, 2^n - 2)$ could be used as a key.

2.4.2 Massey-Omura Scheme or Three-Pass System [14, 15]

Consider n which is a prime or a product of large primes. Suppose user A wishes to send a message $m \in Z_n$. Then the encryption is given by A selecting a random c satisfying

$$0 < c < n \text{ and } gcd(c, n) = 1$$

and she transmits to B

$$c_1 \equiv m^c \pmod n \qquad (2.4.10)$$

Now B chooses a random integer d with the same properties, and transmits

$$\begin{aligned} c_2 &\equiv c_1^d \pmod n \\ &\equiv (m^c)^d \pmod n \\ &\equiv m^{cd} \pmod n \end{aligned} \tag{2.4.11}$$

Then A transmits back to B

$$c_3 \equiv c_2^{c'} \tag{2.4.12}$$

where $c' \in Z_n$ such that $cc' \equiv 1 \pmod{\phi(n)}$ or

$$\begin{aligned} c_3 &\equiv (c_1^d)^{c'} \pmod n \\ &\equiv (m^{dc})^{c'} \pmod n \\ &\equiv m^d \pmod n \end{aligned} \tag{2.4.13}$$

Finally B computes

$$c_4 \equiv c_3^{d'} \pmod n \tag{2.4.14}$$

where $dd' \equiv 1 \pmod{\phi(n)}$ or

$$\begin{aligned} c_4 &\equiv m^{dd'} \pmod n \\ &\equiv m \pmod n \end{aligned} \tag{2.4.15}$$

This scheme retains all the advantages of Pohlig-Hellman scheme. However, the requirement that A and B need to communicate three times over to get a message m transmitted from one to another may not be suitable for many practical purposes.

2.4.3 Rivest-Shamir-Adleman (RSA) Scheme

This scheme [5, 10, 15] runs similar to the previous schemes i.e the enciphering and deciphering functions are given by

$$c \equiv m^e \pmod n \tag{2.4.16}$$

$$m \equiv c^d \pmod{n} \tag{2.4.17}$$

Here, the modulus n is the product of two large primes p and q

$$n = pq \tag{2.4.18}$$

and thus

$$\phi(n) = (p-1)(q-1) \tag{2.4.19}$$

Rivest, Shamir, and Adleman recommment picking d relatively prime to $\phi(n)$ in the interval $(max(p,q)+1, n-1)$.

Because $\phi(n)$ cannot be determined without knowing the prime factors p and q, it is possible to keep d secret even if e and n are made public. This means that the RSA scheme can be used for public-key encryption, where the enciphering transformation is made public and the deciphering transformation is kept secret.

The security of the system depends on the difficulty of factoring n into p and q. The known factoring algorithm, due to Schroppel [10] takes

$$T = exp(sqrt(lnp(lnln(n)))\text{ steps} \tag{2.4.20}$$

2.5 Discrete Logarithm problem and recent advances in breaking ciphers

Several problems in number theory are believed to be computationally intractible, a property that is potentially of great use in cryptography. Included in this category are problems related to integer factorization and the evaluation of discrete logarithms in various groups. We shall consider the discrete logarithm problem over groups.

Let G be a finite cyclic group, and let α be a generator for G. Let $\#G$ be the order of G. The discrete logarithm of an element β to the base α in G is an integer x such that

$$\alpha^x = \beta \tag{2.5.1}$$

If x is restricted to the interval $0 \leq x \leq \#G$, then the discrete logarithm of β to the base α is unique. We write

$$x = log_{\alpha}\beta \tag{2.5.2}$$

The discrete logarithm problem is to find a computationally feasible method to find logarithms in a given group G [2, 4, 9, 11, 15, 19].

For groups having small orders, one method to solve this problem is to precompute a table of logarithms in one go. Another is to compute consecutive powers of α and compare with β till a match is found. But these primitive methods are impractical when $\#G$ is sufficiently large [2].

Several other methods have been developed to find order $\#G$ for large values in subexponential times - Baby-Step Giant-Step method [13], Pollard's ρ method [21], Pohlig-Hellman [19] etc. The most powerful method evolved as yet for computing logarithms over cyclic groups is Index Calculus method [2, 4, 15]. The underlying philosophy in all these methods is that they exploit the multiplicative nature of the group where discrete logarithms are to be computed. As an example, we shall briefly discuss the generic description of the Index Calculus Method.

Let G be a finite cyclic group of order $\#G$ generated by α in which we wish to compute logarithms to the base α. Suppose $\Omega = \{p_1, p_2, \cdots, p_n\}$ be a subset of G with the property that a *significant* fraction of all elements of G can be written as a product of elements from Ω. The set Ω is called the *factor base* for the index calculus method.

In Stage I, we attempt to find the logarithm of all the elements of Ω. We pick a random integer a and attemptt to write α^a as a product of the elements in Ω,

$$\alpha^a = \prod_{i=1}^{t} p_i^{\beta_i} \tag{2.5.3}$$

If we are successful, then the above equation yields a congruence relationship

$$a \equiv \sum_{i=1}^{t} \beta_i log_{\alpha} p_i \pmod{\#G} \tag{2.5.4}$$

This way we collect relations greater than t to form a set of equations which are expected to have a unique solution for the indeterminates $log_{\alpha}p_i \; \forall i \in \{1, 2, \cdots, t\}$.

In Stage II, we compute the individual logarithms in G. Given an element $\delta \in G$, we wish to find an integer x such that

$$\alpha^x = \delta \tag{2.5.5.a}$$

or equivalently,

$$x = log_{\alpha}\delta \tag{2.5.5.b}$$

For this, we pick up random integers s until $\alpha^s\delta$ can be written as a product of elements in Ω

$$\alpha^s\delta = \prod_{i=1}^{t} p_i^{b_i} \tag{2.5.6}$$

We then have

$$log_{\alpha}\delta \equiv \sum_{i=1}^{t} b_i log_{\alpha}p_i - s \pmod{\#G} \tag{2.5.7}$$

The suitability of the above method depends critically on the fact that we need to select an *appropriate* set Ω, and how to generate the other relations *efficiently* †.

Unfortunately, it is found that groups based on multiplication operation *i.e* multiplicative groups are easily amenable to such requirements and thus the Index Calculus Method (and similarly other methods like Pohlig-Hellman,etc. mentioned above, which also require a precomputed factor database) work fairly efficiently. Thus traditional cryptographic schemes like Diffie-Hellman, Pohlig-Hellman, El Gamal, etc based on finite fields and whose security is based on computing discrete logarithms over finite multiplicative groups thus become targets of cryptanalytic attacks based on above techniques.

So, an obvious way to ward off these attacks are to look for such finite groups G where finding logarithms of elements is infeasible. The groups that have been considered are Jacobian of a hyperelliptic curve defined over a finite field, the group of non-singular

† *by that we mean that the set Ω is small and at the same time the proportion of elements in G that factor in Ω is large.*

matrices over a finite field, the class group of an imaginary quadratic field, group of points on an elliptic curve over a finite field. Among these algebraic groups, the elliptic curve groups [2, 14, 17] and non-singular matrix groups [22] have been considered for cryptographic implemention. In our analysis, we shall study the elliptic curve groups for defining cryptosystems and try to base the security of the existing public-key cryptosystems like Pohlig-Hellman, El Gamal, etc. on the elliptic curve discrete logarithm problem. These groups have the advantage that the above methods of discrete logarithm computations do not seem to generalize to them, and if the order of the group is properly chosen, then the discrete logarithm problem can be made extremely difficult to compute.

Chapter 3
Elliptic Curve Structures over Finite Fields

3.1 Introduction

The group of points on an elliptic curve over any arbitrary field can be defined as the set of solutions (x, y) of a certain third-order algebraic equation.

Definition: [2, 6, 14, 17, 21] *An elliptic curve $E(F_k)$ over a field F_k is defined to consist of all points $(x, y) \in F_k \times F_k$ which are the solutions of the Weirstrass Equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.1.1}$$

where $a_i \in F_k$ for $i \in Z$ such that $E(F_k)$ has no singularities (discussed later).

Define the quantities

$$\begin{aligned} d_2 &= a_1^2 + 4a_2 \qquad (3.1.2)\\ d_4 &= 2a_4 + a_1a_3 \\ d_6 &= a_3^2 + 4a_6 \\ d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ c_4 &= d_2^2 - 24d_4 \end{aligned}$$

and

$$\begin{aligned} \Delta &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \qquad (3.1.3)\\ j(E) &= \frac{c_4^3}{\Delta} \end{aligned}$$

The quantity Δ is called the discriminant of the Weirstrass equation and $j(E)$ is called the j-invariance of E if $\Delta \neq 0$ [2, 3, 6, 14, 17, 21]. The following theorems explain the significance of these quantities.

Theorem 3.1.1 *Let E be the given Weirstrass equation (3.1.1). Then E is an elliptic curve, i.e., the Weirstrass equation is non-singular if and only if $\Delta \neq 0$.*

Theorem 3.1.2 *Two elliptic curves $E_1(F_k)$ and $E_2(F_k)$ given by the non-singular Weirstrass equations*

$$E_1 : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6' \tag{3.1.1.a}$$

$$E_1 : y^2 + a_1''xy + a_3''y = x^3 + a_2''x^2 + a_4''x + a_6'' \tag{3.1.1.b}$$

are isomorphic over F_k, denoted by $E_1 \cong E_2$, if and only if there exist variables $u, r, s, t \in F_k, u \neq 0$, such that the change of variables

$$(x, y) \longrightarrow (u^2x + r, u^3y + u^2sx + t) \tag{3.1.4}$$

transforms equation E_1 to equation E_2. The relation of isomorphism is an equivalence relation.

Theorem 3.1.3 *If two elliptic curves $E_1(F_k)$ and $E_2(F_k)$ are isomorphic over F_k, then $j(E_1) = j(E_2)$. If two elliptic curves are isomorphic, then they are also isomorphic as abelian groups. The converse statement is not true in general.*

For various characteristics of the field F_k denoted by $char(F_k)$, the above equation can be reduced by means of coordinate transformation.

a) Case when curve over F_k, $char(F_k) \neq 2, 3$

If $char(F_k) \neq 2$, then by means of the following transformation on eq. (3.1.1),

$$(x, y) \longrightarrow (x, y - \frac{a_1x}{2} - \frac{a_3}{2}) \tag{3.1.5}$$

we get,

$$E' : y^2 = x^3 + b_2x^2 + b_4x + b_6 \tag{3.1.6}$$

where

$$\begin{aligned} b_2 &= a_2 + \frac{a_1^2}{4} \\ b_4 &= a_4 + \frac{a_1a_3}{2} \\ b_6 &= a_6 + \frac{a_3^2}{4} \end{aligned} \tag{3.1.7}$$

$E(F_k)$ is isomorphic to $E'(F_k)$ over F_k ,or

$$E(F_k) \cong E'(F_k) \text{ over } F_k \tag{3.1.8}$$

Since $char(F_k) \neq 2, 3$, then further change of variables

$$(x, y) \longrightarrow (\frac{x - 12b_2}{36}, \frac{y}{216}) \tag{3.1.9}$$

we get,

$$E'' : y^2 = x^3 + ax + b \tag{3.1.10}$$

where

$$\begin{aligned} a &= -432b_2^2 + 1296b_4 \\ b &= 46656b_6 - 15552b_2b_4 + 3456b_2^3 \end{aligned} \tag{3.1.11}$$

Again $E'(F_k) \cong E''(F_k)$ over F_k.

Hence $E(F_k) \cong E''(F_k)$ over F_k.

Theorem 3.1.4 *The elliptic curves*

$$E_1(F_k) : y^2 = x^3 + a'x + b' \tag{3.1.12}$$

$$E_2(F_k) : y^2 = x^3 + a''x + b'' \tag{3.1.13}$$

are isomorphic over F_k if and only if there exists a $u \in F_k$ such that

$$\begin{aligned} u^4a'' &= a' \\ u^6b'' &= b' \end{aligned} \tag{3.1.14}$$

If $E_1(F_k) \cong E_2(F_k)$ over F_k, then the isomorphism relation is given by

$$\chi : E_1 \longrightarrow E_2, \; \chi : (x, y) \longrightarrow (u^{-2}x, u^{-3}y) \tag{3.1.15.a}$$

or equivalently,

$$\psi : E_2 \longrightarrow E_1, \ \ \psi : (x, y) \longrightarrow (u^2x, u^3y) \tag{3.1.15.b}$$

For the elliptic curve $E''(F_k)$,given by eq (3.1.10), the associated discriminant Δ and j-invariant $j(E_k)$ over F_k are given by

$$\Delta = -16(4a^3 + 27b^2) \tag{3.1.16}$$

and

$$j(E_k) = -\frac{1728(4a)^3}{\Delta} \tag{3.1.17.a}$$

b) Case when curve over F_k, $char(F_k) = 2$

Consider $E(F_k)$ given by the general Weirstrass equation,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.1.1}$$

Using equation (3.1.2), we calculate the j-invariance for $char(F_k) = 2$ as

$$j(E_k) = \frac{a_1^{12}}{\Delta} \tag{3.1.17.b}$$

There could be two kinds of curves defined for this case [2, 13].

1) Case when j-invariance equals zero

Since $j(E_k) = 0$, we have $a_1 = 0$. Consider the following transformation

$$\theta : (x, y) \longrightarrow (x + a_2, y) \tag{3.1.18}$$

We get

$$E_2 : y^2 + a_3'y = x^3 + a_4'x + a_6' \tag{3.1.19}$$

Here $E(F_k) \cong E_2(F_k)$.

The above curve is called j-invariant curve over F_k, $char(F_k) = 2$.

2) Case when j-invariance is not equal to zero

Consider the following transformation of equation 3.1.1 and assuming $char(F_k) = 2$

$$\xi : (x, y) \longrightarrow (a_1^2 x + \frac{a_3}{a_1}, a_1^3 y + \frac{a_1^2 + a_3^2}{a_1^3}) \tag{3.1.20}$$

We get

$$E_2 : y^2 + xy = x^3 + a_2 x^2 + a_6 \tag{3.1.21}$$

The above curve is called j-variant curve over F_k, $char(F_k) = 2$.

3.2 The Elliptic Curve Group Algebra

The points on an elliptic curve alongwith a special point (∞, ∞) denoted by $\underline{O}$ (the identity element) form an abelian group under a certain addition operation given by $\oplus$ [2, 3, 6, 12, 13, 16, 21] . Let $E(F_k)$ be an elliptic curve defined by the Weirstrass equation (3.1.1). The rules of addition are given as following :-

Consider two points $P, Q \in E(F_k)$. Then,

a) $\underline{O} \oplus P = P$ and $P \oplus \underline{O} = P$.

b) $-\underline{O} = \underline{O}$.

c) If $P = (x_1, y_1) \neq \underline{O}$, then $-P = (x_1, -y_1 - a_1 x_1 - a_3)$.

d) If $Q = -P$, then $P \oplus Q = \underline{O}$.

e) If $P \neq \underline{O}, Q \neq \underline{O}, Q \neq -P$, then let R be the third point of intersection of either the line $\overline{PQ}$ if $P \neq Q$ or the tangent line to the curve at P if $P = Q$, with the curve. Then, $P \oplus Q = -R$.

Explicit formulae for the group operation $\oplus$ is defined as following. Consider $P = (x_1, y_1), Q = (x_2, y_2)$ and let $P \oplus Q = (x_3, y_3)$ be points on the general elliptic curve equation given below

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \tag{3.1.1}$$

Define

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{if } P \neq Q \\ \dfrac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}, & \text{if } P = Q. \end{cases} \tag{3.2.1}$$

Table 1: Cayley Table illustrating Abelian Group formed by the elliptic curve E $y^2+y = x^3$ over the field F_{2^3}

$\oplus$	$(1,\alpha^3$ †$)$	$(1,\alpha^2)$	(α^3,α^5)	(α^3,α)	(α^5,α^7)	$(\alpha^5,1)$	(α^6,α^6)	(α^6,α^4)	(∞,∞)
$(1,\alpha^3)$	$(1,\alpha^2)$	(∞,∞)	(α^6,α^6)	$(\alpha^5,1)$	(α^3,α^5)	(α^6,α^4)	(α^5,α^7)	(α^3,α)	$(1,\alpha^3)$
$(1,\alpha^2)$	(∞,∞)	$(1,\alpha^2)$	(α^5,α^7)	(α^6,α^4)	(α^6,α^6)	(α^3,α)	(α^3,α^5)	$(\alpha^5,1)$	$(1,\alpha^2)$
(α^3,α^5)	(α^6,α^6)	(α^5,α^7)	$(\alpha^5,1)$	(∞,∞)	(α^3,α)	$(1,\alpha^3)$	(α^6,α^4)	$(1,\alpha^2)$	(α^3,α^5)
(α^3,α)	$(\alpha^5,1)$	(α^6,α^4)	(∞,∞)	(α^5,α^7)	$(1,\alpha^2)$	(α^3,α^5)	$(1,\alpha^3)$	(α^6,α^6)	(α^3,α)
(α^5,α^7)	(α^3,α^5)	(α^6,α^6)	(α^3,α)	$(1,\alpha^2)$	(α^6,α^4)	(∞,∞)	$(\alpha^5,1)$	$(1,\alpha^3)$	(α^5,α^7)
$(\alpha^5,1)$	(α^6,α^4)	(α^3,α)	$(1,\alpha^3)$	(α^3,α^5)	(∞,∞)	(α^6,α^6)	$(1,\alpha^2)$	(α^5,α^7)	$(\alpha^5,1)$
(α^6,α^6)	(α^5,α^7)	(α^3,α^5)	(α^6,α^4)	$(1,\alpha^3)$	$(\alpha^5,1)$	$(1,\alpha^2)$	(α^3,α)	(∞,∞)	(α^6,α^6)
(α^6,α^4)	(α^3,α)	$(\alpha^5,1)$	$(1,\alpha^2)$	(α^6,α^6)	$(1,\alpha^3)$	(α^5,α^7)	(∞,∞)	(α^3,α^5)	(α^6,α^4)
(∞,∞)	$(1,\alpha^3)$	$(1,\alpha^2)$	(α^3,α^5)	(α^3,α)	(α^5,α^7)	$(\alpha^5,1)$	(α^6,α^6)	(α^6,α^4)	(∞,∞)

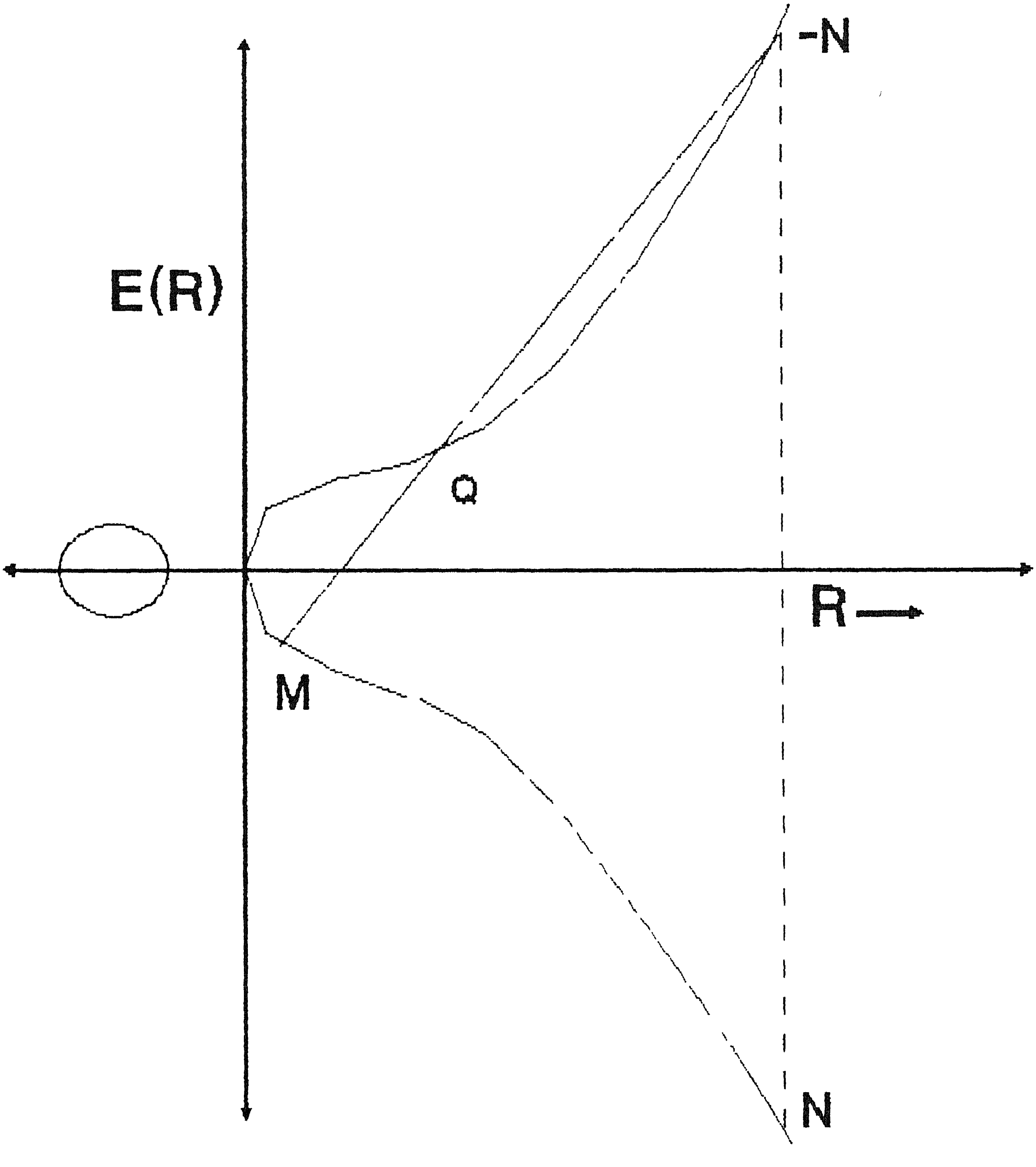
† *α is a primitive root of the irreducible polynomial $f(x) = x^3 + x^2 + 1$ which generates F_{2^3} i.e* $f(\alpha) = 0$

FIG. 3:

GEOMETRIC INTERPRETATION OF GROUP OPERATION

OF ELLIPTIC CURVE {E,(+)} DEFINED OVER

SET OF REALS R , M (+) Q = N



Let $\varphi = y_1 - \lambda x_1$.

Then,

$$x_3 \overset{\text{def}}{=} \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \tag{3.2.2}$$

$$y_3 \overset{\text{def}}{=} -(\lambda + a_1)x_3 - \varphi - a_3 \tag{3.2.3}$$

To illustrate the addition law, let us consider the following examples.

Example: Assume an elliptic curve

$$E : y^2 = x^3 - 16x + 16$$

defined over Q, the set of rationals. The point $P = (0, 4)$ satisfies the above equation. To obtain $2P = P \oplus P$, we invoke the above formula (for $P = Q$ case) to obtain $\lambda = -2$ from which we get $2P = (4, 4)$. From P and $2P$, we obtain $3P$ (using $P \neq Q$ case) as $3P = (-4, -4)$. Continuing this way, higher multiples of P are: $4P = (8, -20), 5P = (1, -1), 6P = (24, 116), 7P = (\frac{-20}{9}, \frac{-308}{27}), \cdots$

Example: Consider an elliptic curve $E : y^2 + y = x^3$ defined over $\frac{F_{2^3}}{f(x)}$ where $f(x)$ is the irreducible polynomial $x^3 + x^2 + 1$ which defined the field F_{2^3}. Let α be a primitive root of the polynomial *i.e* $f(\alpha) = 0$. Consider the Cayley Table (see Table 1) formed by the points of the above elliptic curve with a defined operation $\oplus$. It can be easily verified that with the above operation $\{E(F_k), \oplus\}$ forms an abelian group.

The above explanation is best illustrated with the field $F = \Re$, the set of real numbers as shown in Figure 3.

The line joining the points P_1 and P_2 has a gradiant λ given by the above formula; the alternative is derived from the limiting case when the chord becomes the tangent at P_1. This line intersects the curve at one further point P', whose negative is defined to be the sum of P_1 and P_2.

One way of interpreting the addition law on $E(F_k)$ is to state that the three points P, Q, R are colinear if and only if

$$P \oplus Q \oplus R = \underline{O} \tag{3.2.4}$$

With this interpretation, the condition for non-singularity (Theorem 3.1.1) can be interpreted as - the cubic in x should not have a linear factor squared. This is easier understood by the geometrical implications - having a double root means that the slope of the curve $E(F_k)$ is not well defined at that double point.

Let us consider an elliptic curve (defined over a field with characteristic $\neq 2,3$) having double root at $x \equiv -\alpha \pmod{k}$.

$$y^2 = (x+\alpha)^2(x+\beta) \tag{3.2.5}$$
$$y^2 = x^3 + (2\alpha+\beta)x^2 + (\alpha^2+2\alpha\beta)x + \alpha^2\beta$$

Comparing with $y^2 = x^3 + ax + b$, we get

$$2\alpha + \beta = 0 \tag{3.2.6}$$
$$a = \alpha^2 + 2\alpha\beta$$
$$b = \alpha^2\beta$$

and $4a^3 + 27b^2 = 0$. Hence the condition for non-singularity is

$$\Delta = -16(4a^3 + 27b^2) \neq 0 \tag{3.2.7}$$

3.2.1 Elliptic curve over field of characteristic $char(E(F_k)) > 3$

The elliptic curve equation can be written as

$$E : y^2 = x^3 + ax + b \tag{3.2.8}$$

Using Equations (3.2.1), (3.2.2), (3.2.3) and comparing with (3.2.8), we get the addition formula as following

If $P = (x_1, y_1) \in E$, then $-P = (x_1, -y_1)$ and $P \oplus (-P) = \underline{O}$. Given another point $Q = (x_2, y_2) \in E$, it satisfies the above properties and if $Q \neq -P$, then $P \oplus Q = (x_3, y_3)$ where

$$x_3 = \lambda^2 - x_1 - x_2 \tag{3.2.9}$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$

where

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{if } P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1}, & \text{if } P = Q \end{cases} \tag{3.2.10}$$

Example: Consider the following example to illustrate abelian group induced by an elliptic curve over a field F_5

$$y^2 = x^3 + 2 \tag{3.2.11}$$

Here the co-ordinates defining the elliptic curve group are :

$(2,0),(3,2),(3,3),(4,1),(4,4),(\infty,\infty) = \underline{Q}$ which is the zero of the group. Order of the above group is 6. The order of each of the group elements is calculated as follows :-

i) Consider $Q = (2,0)$.

$$Q \oplus Q = (2,0) \oplus (2,0) = (\infty,\infty)$$

Hence $2Q = \underline{Q}$.

ii) Consider $Q = (3,2)$.

$$Q \oplus Q = (3,2) \oplus (3,2) = (3,3)$$

$$2Q \oplus Q = (3,3) \oplus (3,2) = (\infty,\infty)$$

Hence $3Q = \underline{Q}$.

iii) Consider $Q = (3,3)$

$$Q \oplus Q = (3,3) \oplus (3,3) = (3,2)$$

$$2Q \oplus Q = (3,2) \oplus (3,3) = (\infty,\infty)$$

Hence $3Q = \underline{Q}$.

iv) Consider $Q = (4,1)$

$$Q \oplus Q = (4,1) \oplus (4,1) = (3,3)$$

$$2Q \oplus Q = (3,3) \oplus (4,1) = (2,0)$$

$$3Q \oplus Q = (2,0) \oplus (4,1) = (3,2)$$

$$4Q \oplus Q = (3,2) \oplus (4,1) = (4,4)$$

$$5Q \oplus Q = (4,4) \oplus (4,1) = (\infty,\infty)$$

Hence $6Q = \underline{O}$.

v) Consider $Q = (4,4)$

$$\begin{aligned} Q \oplus Q &= (4,4) \oplus (4,4) = (3,2) \\ 2Q \oplus Q &= (3,2) \oplus (4,4) = (2,0) \\ 3Q \oplus Q &= (2,0) \oplus (4,4) = (3,3) \\ 4Q \oplus Q &= (3,3) \oplus (4,4) = (4,1) \\ 5Q \oplus Q &= (4,1) \oplus (4,4) = (\infty,\infty) \end{aligned}$$

Hence $6Q = \underline{O}$.

3.2.2 Elliptic curve over field of characteristic $char(E(F_k)) = 2$

Here we shall consider two cases

a) j-invariant elliptic curves $(j(E(F_k)) = 0)$.

b) j-variant elliptic curves $(j(E(F_k)) \neq 0)$.

For case a), the elliptic curve equation can be written as

$$E : y^2 + a_3y = x^3 + a_4x + a_6 \tag{3.2.12}$$

Using Equations (3.2.1), (3.2.2), (3.2.3) and comparing with (3.2.12), we get the addition formula as following :-

If $P = (x_1, y_1) \in E$, then $-P = (x_1, y_1 + a_3)$ and $P \oplus (-P) = \underline{O}$. Given another point $Q = (x_2, y_2) \in E$, it satisfies the above properties and if $Q \neq -P$, then $P \oplus Q = (x_3, y_3)$ where

$$x_3 = \begin{cases} \left(\dfrac{y_2 + y_1}{x_2 + x_1}\right)^2 + x_1 + x_2, & \text{if } P \neq Q \\ \dfrac{x_1^4 + a_4^2}{a_3^2}, & \text{if P = Q} \end{cases} \tag{3.2.13}$$

and

$$y_3 = \begin{cases} \left(\dfrac{y_2 + y_1}{x_2 + x_1}\right)(x_1 + x_3) + y_1 + a_3, & \text{if } P \neq Q \\ \left(\dfrac{x_1^2 + a_4}{a_3}\right)(x_1 + x_3) + y_1 + a_3, & \text{if } P = Q \end{cases} \tag{3.2.14}$$

For case b), the elliptic curve equation can be written as

$$E : y^2 + xy = x^3 + a_4x + a_6 \tag{3.2.15}$$

Using Equations (3.2.1), (3.2.2),(3.2.3) and comparing with(3.2.15), we get the addition formula as following :-

If $P = (x_1, y_1) \in E$, then $-P = (x_1, y_1 + a_3)$ and $P \oplus (-P) = \underline{Q}$. Given another point $Q = (x_2, y_2) \in E$, it satisfies the above properties and if $Q \neq -P$, then $P \oplus Q = (x_3, y_3)$ where

$$x_3 = \begin{cases} \left(\dfrac{y_2 + y_1}{x_2 + x_1}\right)^2 + \dfrac{y_1 + y_2}{x_1 + x_2} + x_1 + x_2 + a_2, & \text{if } P \neq Q \\ x_1^2 + \dfrac{a_6}{x_1^2}, & \text{if } P = Q. \end{cases} \tag{3.2.16}$$

and

$$y_3 = \begin{cases} \left(\dfrac{y_2 + y_1}{x_2 + x_1}\right)(x_1 + x_3) + y_1 + x_3, & \text{if } P \neq Q \\ x_1^2 + \left(x_1 + \dfrac{y_1}{x_1}\right)x_3 + x_3, & \text{if } P = Q \end{cases} \tag{3.2.17}$$

3.2.3 Properties of Elliptic Curves defined over a field F_k

Theorem 3.2.1: *(Hasse [6, 14, 21]) Let $\#E(F_k)$ be the order of an elliptic curve group $E(F_k)$ defined over a field F_k with k elements. Then*

$$(\sqrt{k} - 1)^2 \leq \#E(F_k) \leq (\sqrt{k} + 1)^2 \tag{3.2.18.a}$$

or

$$\#E(F_k) = k + 1 + a_k \tag{3.2.18.b}$$

where $k + 1$ is the expected number of solutions and a_k is the discrepency as (by Riemann Hypothesis for Abelian Variants of dimension 1)

$$|a_k| \leq 2\sqrt{k} \tag{3.2.18.c}$$

Theorem 3.2.2: *(Cassels [6], [21]) The group $E(F_k)$ is either cyclic or the product of two cyclic groups of order m_1 and m_2 satisfying*

$$m_1|m_2, \qquad m_1|gcd(m, k-1) \tag{3.2.19}$$

where $m = \#E(F_k)$ and F_k has k elements.

Corollary: *If $\#E(F_k)$ is squarefree, then surely $E(F_k)$ is cyclic.*

Remark: *Similarly for the other case, if $\#E(F_k)$ is non-squarefree, then $E(F_k)$ need not be a cyclic group.*

Consider $m = \#E(F_k)$ to be a square i.e $m = p_1^2$ where p_1 is a prime number. Assume that the group has the order m of the form $(\sqrt{k}+1)^2$ (this satisfies Theorem 3.2.1).

$$\begin{aligned}(\sqrt{k}+1)^2 &= p_1^2 \\ k &= (p_1-1)^2\end{aligned} \tag{3.2.20}$$

and

$$\begin{aligned}gcd(m, k-1) &= gcd(p_1^2, k-1) \\ &= gcd((\sqrt{k}+1)^2, k-1)\end{aligned} \tag{3.2.21}$$

which is greater than 1. Here the group is a product of two cyclic groups. Hence, our assertion is proved.

3.3 Classes of Elliptic Curves used for implementation purposes

Certain classes of elliptic curves are of special interest to our work [3, 16]. We shall discuss their properties.

Theorem 3.3.1: *Let p be an odd prime satisfying*

$$p \equiv 2 \pmod 3 \tag{3.3.1}$$

Then for $0 < b < p$, *and* $a = 0$, $E(Fp)$ *is a cyclic group of order*

$$\#E(F_p) = p + 1 \tag{3.3.2}$$

Proof:

$$E(Fp) : y^2 = x^3 + b \tag{3.3.3}$$

For $p \equiv 2 \pmod 3$, the mapping $x \longrightarrow x^3$ is a permutation in F_p. Therefore for every b, there are exactly $\dfrac{p-1}{2}$ numbers $x \in F_p$ such that $(x^3 + b)$ is a quadratic residue and for each such x, there are two points on $E(F_p)$ viz. $(x, \pm\sqrt{x^3 + b})$. This combined with the point $(-b^{\frac{1}{3}}, 0)$ and $\underline{O}$, there are $(p + 1)$ points on $E(F_p)$.

To prove that $E(F_p)$ is cyclic , assume it is not cyclic.Then,

$$E(F_p) \cong Z_{N_1} \times Z_{N_2} \tag{3.3.4}$$

where $N_1.N_2 = p + 1$ and $N_1 | N_2$ and $N_1 | gcd(p + 1, p - 1)$.

Now, N_1 equals 2 and N_2 is even. Thus the group $Z_{N_1} \times Z_{N_2}$ must have four elements such that $-P = P$. However there are only two points $P = O$ and $P = (-b^{\frac{1}{3}}, 0)$ for which $-P = P$, since the only points where $-P = P$ are the points (x, y) with $y = 0$. This contradicts our assumption and hence proved.

Theorem 3.3.2: *Let* p *be a prime satisfying* $p \equiv 3 \pmod 4$. *Then, for* $0 < a < p$, *we have*

$$\#E(F_p) = p + 1 \tag{3.3.5}$$

Moreover, $E(F_p)$ is cyclic if a is a quadratic residue modulo p and $E(F_p) \cong Z_{\frac{p+1}{2}} \times Z_2$ otherwise.

Theorem 3.3.3: *Let* m *be an odd positive integer greater than* q. *Then the elliptic curve group defined by*

$$E(F_{2^m}) : y^2 + y = x^3 + b \tag{3.3.6}$$

has $2^m + 1$ *solutions.*

Proof: By an arguement similar to the one given in Theorem 3.3.1, $x \longrightarrow x^3 + b$ is a permutation polynomial over F_2^m and exactly half the elements i.e 2^{m-1} have trace function (discussed in next section) equal to 0. Therefore, solutions for the quadratic equation given by Equation (3.3.6) exists for 2^{m-1} cases. Hence total number of solutions is $2.2^{m-1} = 2^m$ and including the identity element of the group O, we have in all $2^m + 1$ solutions.

To avoid cumbersome computations, it is suggested to use the following subclass of elliptic curves. For $char(F_k) = 2$, $k = 2^m$,

a) j-invariant class

$$E_1 : y^2 + y = x^3 + b \tag{3.3.7}$$

Since the order of the above elliptic curve group is given by $\#E(F_{2^m}) = 2^m + 1$, and since 2 does not divide $2^m + 1$, we could choose $2^m + 1 = 3.p^*$ where p^* is a large prime.

b) j-variant class

$$E_2 : y^2 + xy = x^3 + b \tag{3.3.8}$$

Here, the choice of m being odd is also advantageous since it is easy to recover the y-coordinate of a point given its x-coordinate (this is discussed in detail later in the text). This helps in reducing message expansion when ciphertext is encrypted.

Curves over F_{2^m} with zero j-invariance are preferred since

i) Arithmetic over F_{2^m} is easier to implement in normal basis representation (discussed later) since a squaring operation is equivalent to a simple left shift operation.

ii) For doubling operation, further reduction in computation is achieved by choosing $a_3 = 1$ by which inversion operation at each step is eliminated.

There are three useful classes of curves over F_{2^m} with m being odd

$$\begin{aligned} &y^2 + y = x^3 && (3.3.7.a)\\ &y^2 + y = x^3 + x\\ &y^2 + y = x^3 + x + 1 \end{aligned}$$

For $char(F_k) > 3$, we use

$$E_3 : y^2 = x^3 + b \tag{3.3.9}$$

Since the above elliptic group has an order $\#E(F_k) = p + 1$ for $p \equiv 2 \pmod 3$, and p being odd, we have $3|(p+1)$ and $2|(p+1)$. Hence for encryption purposes, we may choose p as follows. Choose $(p+1) = 2.3.p^*$ where p^* is another large prime. Therefore $p = 2.3.p^* + 1$.

The motivation of adopting such a scheme is that given an elliptic curve with coefficients arbitrarily chosen from the field F_k over which it is defined, the best algorithms for computing the order of the group [13], in addition to being complicated, have a running time $O(log^9 q)$, where q is the largest prime factor of the order of the group $\#E(F_k)$. The probabilistic nature of the algorithm renders it unsuitable for implementation purposes.

3.4 Message Embedding Schemes

From a practical viewpoint, the first step is to find the points of a given elliptic curve defined over a specified field F_k having characteristic denoted by $char(F_k)$. We shall discuss two cases

a) the general case of field F_k having $char(F_k) > 3$

b) the specific case of field F_k with $char(F_k) = 2, k = 2^n$, n being an odd integer.

3.4.1 Implementation over fields of characteristic > 3

We define the elliptic curve E_1 as

$$E_1 : y^2 = x^3 + ax + b \tag{3.4.1}$$

Note that the general Weirstrass equation given by equation (3.1.1) is isomorphic to E_1 as defined above

We start with the concept of quadratic residue.

Definition: [18] *Let $m > 1$ be a fixed integer An integer a with $gcd(a, m) = 1$ is called a quadratic residue modulo m if the congruence equation*

$$x^2 \equiv a \pmod m \tag{3.4.2}$$

FIG. 4: PROCEDURE FOR FINDING SOLUTIONS FOR E(GF(p))

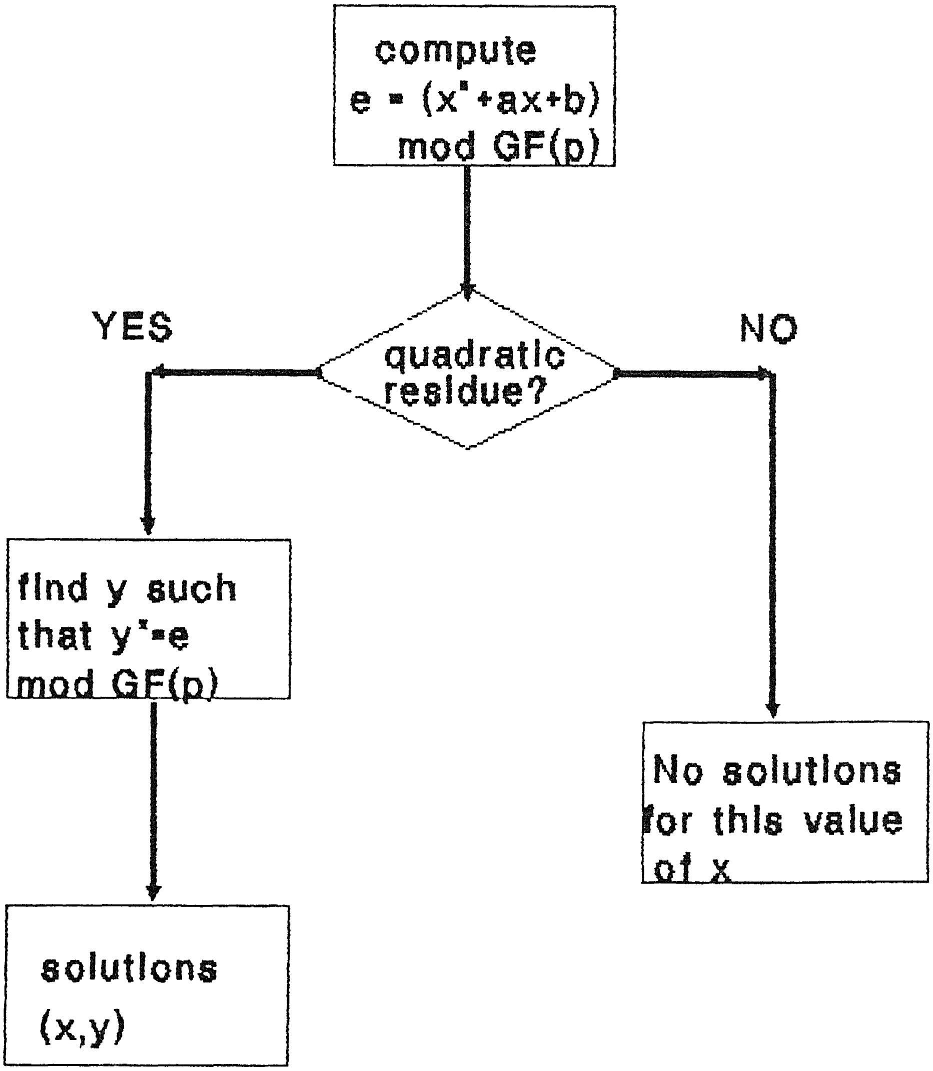


Table 2: Abelian Group formed by Elliptic Curve E $y^2 = x^3 + 1$ over the field F_{79}

(0 , 24)	(0 , 55)
(1 , 19)	(1 , 60)
(2 , 28)	(2 , 51)
(4 , 31)	(4 , 48)
(5 , 4)	(5 , 75)
(6 , 7)	(6 , 72)
(9 , 25)	(9 , 54)
(11 , 20)	(11 , 59)
(13 , 26)	(13 , 53)
(15 , 0)	(17 , 0)
(16 , 30)	(16 , 49)
(19 , 31)	(19 , 48)
(21 , 18)	(21 , 61)
(22 , 28)	(22 , 515)
(24 , 17)	(24 , 62)
(27 , 7)	(27 , 72)
(31 , 34)	(31 , 45)
(32 , 21)	(32 , 58)
(33 , 32)	(33 , 47)
(34 , 15)	(34 , 64)
(35 , 5)	(35 , 74)
(39 , 11)	(39 , 68)
(40 , 2)	(40 , 77)
(42 , 38)	(42 , 41)
(43 , 13)	(43 , 66)
(44 , 10)	(44 , 69)
(46 , 7)	(46 , 72)
(47 , 0)	(∞ , ∞)
(52 , 32)	(52 , 47)
(55 , 28)	(55 , 51)
(56 , 31)	(56 , 48)
(57 , 17)	(57 , 62)
(58 , 14)	(58 , 65)
(62 , 21)	(62 , 58)
(64 , 21)	(64 , 58)
(66 , 9)	(66 , 70)
(67 , 27)	(67 , 52)
(73 , 32)	(73 , 47)
(77 , 17)	(77 , 62)
(78 , 1)	(78 , 78)

has a solution. If equation (3.4.2) has no solution, a is called a quadratic non-residue modulo m.

Theorem 3.4.1: [15, 18] *If p is an odd prime and gcd(a, p) = 1. Then the congruence equation (3.4.2) has two solutions or no solution accordingly as*

$$a^{\frac{p-1}{2}} \equiv +1 \text{ or } -1 \pmod{p} \tag{3.4.3}$$

Example: Consider the field F_7. The elements comprising the multiplicative group are $1, 2, 3, 4, 5$ and 6.

Consider $1^3 \equiv 1, 2^3 \equiv 1, 3^3 \equiv -1, 4^3 \equiv 1, 5^3 \equiv -1, 6^3 \equiv -1$, all evaluated modulo 7. Hence, by the above theorem, $1, 2, 4$ are quadratic residue mod 7 whereas $3, 5, 6$ are quadratic non-residues mod 7. Notice that $1^2 \equiv 6^2 \equiv 1 \pmod{7}$, $3^2 \equiv 4^2 \equiv 2 \pmod{7}$, $2^2 \equiv 5^2 \equiv 4 \pmod{7}$.

We find that there are exactly $\frac{p-1}{2}$ numbers between 1 and p which are quadratic residues modulo p and each one of these quadratic residues have two solutions over F_k.

Hence a general procedure for finding the points of a given elliptic curve defined over a specified field F_k can be depicted as shown in Figure 4.

Example: Consider the abelian group formed by $E : y^2 = x^3 + 1$ over the field F_{79}. Table 2 illustrates the points on $E(F_{79})$ which have been simulated using the above algorithm.

3.4.2 Implementation over fields of characteristic = 2

We shall restrict our attention to elliptic curves of the form given by

$$E_2 : y^2 + a_3 y = x^3 + a_4 x + a_6 \tag{3.4.4}$$

Although this is a specific case of j-invariant elliptic curves, yet the procedure for finding solutions for the j-variant curves proceeds exactly in a similar fashion and the results here can be easily generalised.

Equation (3.4.4) can be considered a general quadratic equation of the form

$$px^2 + qx + r = 0 \tag{3.4.5.a}$$

defined over $F_k, char(F_k) = 2$. Substituting $y = \frac{px}{q}$, the above equation is recast as

$$y^2 + y + \frac{pr}{q^2} = 0 \tag{3.4.5.b}$$

defined over $F_k, char(F_k) = 2$.

Therefore, without loss of generality, we consider only the solutions of equations of the form [7, 20]

$$x^2 + x + l = 0 \tag{3.4.6}$$

defined over $F_k, char(F_k) = 2$. Note that the standard procedure of finding roots for a quadratic equation $px^2 + qx + r = 0$ as $x = \frac{-p \pm \sqrt{p^2 - 4qr}}{2r}$ does not hold good since the denominator $2r \equiv 0$ for $char(F_k) = 2$.

The following theorems become relevent in our discussion.

Theorem 3.4.2: *Every element of the field F_k with $char(F_k) = 2, k = 2^n$ has a square root in F_k.*

Proof: For the case of the zero element, it is its own square root in any field. For the non-zero elements, consider a field F_k with $char(F_k) = 2$ with a primitive element α. Then any element β can be written as α^i for some i. Then $\sqrt{\beta} = \alpha^{\frac{i}{2}}$ if i is even and $\sqrt{\beta} = \alpha^{\frac{k+i}{2}}$ if i is odd. In both cases $\sqrt{\beta} \in F_k$.

Definition: [15] The q-ary trace of an element β of F_{q^m} is the sum

$$trace(\beta) = \sum_{i=0}^{m-1} \beta^{q^i} \tag{3.4.7.a}$$

Assuming α_1, α_2 are the elements of F_{q^m} of characteristic q, $(\alpha_1 + \alpha_2)^{q^n} = {\alpha_1}^{q^n} + {\alpha_2}^{q^n}$ is true. Hence, the q^{th} power of the q-ary trace of β is equal to the q-ary trace of β and thus the q-ary trace is an element of the ground field F_q. If β has m elements in its conjugacy class, then $trace(\beta)$ is the sum of all the elements in the conjugacy class. Otherwise, the number of elements in the conjugacy class divides m, and the number of times each element is added into the trace is given by this ratio.

Hence it follows,

$$trace(\beta+\gamma) = trace(\beta) + trace(\gamma) \tag{3.4.7.b}$$

and that all the conjugates have the same trace.

Example: Consider the trace function for the elements of the field $\frac{F_{2^7}}{x^7+x^3+1}$ which has been simulated for purposes of illustration

Table : Trace Function for elements of the field F_{2^7}

Elements in conjugacy class	Trace Function
1	1
α[†] α^2 α^4 α^8 α^{16} α^{32} α^{64}	0
α^3 α^6 α^{12} α^{24} α^{48} α^{96} α^{65}	0
α^5 α^{10} α^{20} α^{40} α^{80} α^{33} α^{66}	0
α^7 α^{14} α^{28} α^{56} α^{112} α^{97} α^{67}	1
α^{11} α^{22} α^{44} α^{88} α^{49} α^{98} α^{69}	1
α^{13} α^{26} α^{52} α^{104} α^{81} α^{35} α^{70}	0
α^{17} α^{34} α^{68} α^9 α^{18} α^{36} α^{72}	0
α^{19} α^{38} α^{76} α^{25} α^{50} α^{100} α^{73}	1
α^{23} α^{46} α^{92} α^{57} α^{114} α^{101} α^{75}	1
α^{27} α^{54} α^{108} α^{89} α^{51} α^{102} α^{77}	1

Theorem 3.4.3: *The quadratic equation $x^2+x+a=0$ where a is an element of F_{2^m}, has a root in F_{2^m} if and only if the binary trace of a equals zero.*

Proof: Let β be a root of the quadratic equation. Then the binary trace of the quadratic equation evaluated at β gives

$$trace(\beta^2+\beta+a) = trace(0) = 0 \tag{3.4.8}$$

[†] *α is a primitive root of the irreducible polynomial $f(x) = x^7+x^3+1$ which generates F_{2^7} i.e $f(\alpha) = 0$*

Now the traces of β and β^2 are same elements in ground field F_2 and thus,

$$trace(\beta) + trace(\beta^2) = 0 \tag{3.4.9}$$

and therefore $trace(a) = 0$.

Conversely, every β is a zero of $x^2 + x + a$ for some a, i.e. $a = -(\beta + \beta^2)$. There are 2^{m-1} such a with zero trace, and this just enough to form 2^{m-1} equations, each with two roots. This completes the proof.

Coming back to the problem at hand, let α be an element of F_{2^m} and let $trace(\alpha)$ be denoted as $T_2(\alpha)$. Hence,

$$T_2(\alpha) = \sum_{i=0}^{m-1} \alpha^{2^i} \tag{3.4.10}$$

and since $T_2(\alpha) \in F_2$, $T_2(\alpha)$ is either zero or one.

By our discussions above, we find that Equation (3.4.6) has a solution in F_{2^m} if and only if $T_2(l) = 0$.

Theorem 3.4.4: *Let $x_1 \in F_{2^m}$ be one solution of Equation (3.4.6). Then the other solution is given by $1 + x_1$.*

Proof: We have

$$x_1^2 + x_1 + l = 0$$
$$1 + x_1^2 + 1 + x_1 + l = 0$$
$$(1 + x_1)^2 + (1 + x_1) + l = 0$$

which clearly shows that the other solution is given by $1 + x_1$.

Theorem 3.4.5: *Assume Equation (3.4.6) has a solution x_1 in F_{2^m} and m is odd. Then one solution x_1 can be expressed as*

$$\begin{aligned} x_1 &= \sum_{j \in J} l^{2^j} \\ &= \sum_{i \in I} l^{2^i} \end{aligned} \tag{3.4.11}$$

where $I = \{1, 3, \cdots, m-2\}$ and $J = \{0, 2, 4, \cdots m-1\}$.

FIG. 5:

PROCEDURE FOR FINDING SOLUTIONS ON $E(GF(2^n))$

x is an element in $GF(2^n)$

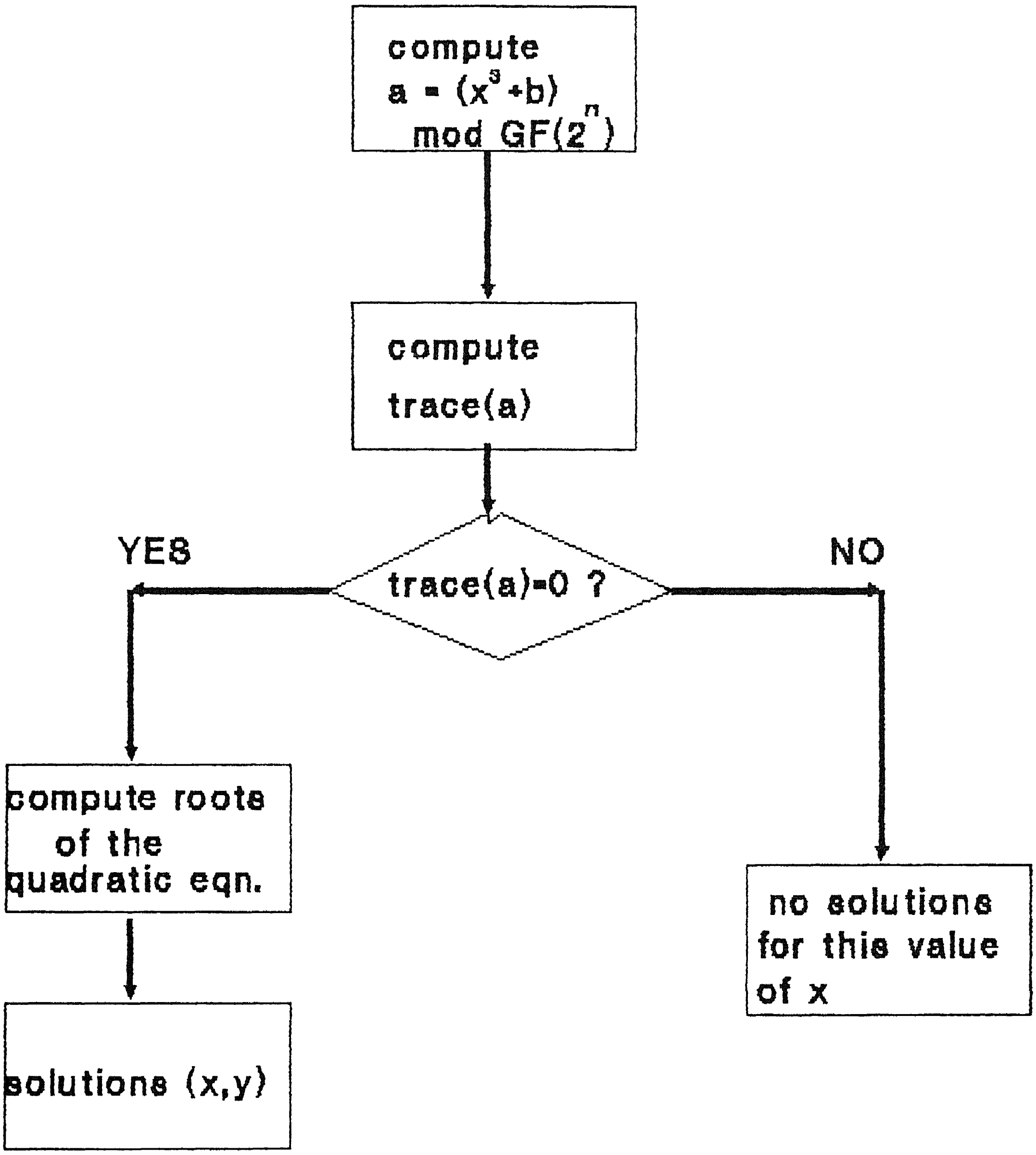


Table 3: Abelian Group formed by j-invariant Elliptic Curve $E \;\; y^2 + y = x^3 + 1$ over the field F_{2^7}

$(\alpha^{1}$ †$, \alpha^{48})$	$(\alpha^{1}, \alpha^{112})$	$(\alpha^{2}, \alpha^{53})$	$(\alpha^{2}, \alpha^{73})$
$(\alpha^{3}, \alpha^{65})$	$(\alpha^{3}, \alpha^{67})$	$(\alpha^{4}, \alpha^{95})$	$(\alpha^{4}, \alpha^{71})$
$(\alpha^{6}, \alpha^{33})$	$(\alpha^{6}, \alpha^{84})$	$(\alpha^{8}, \alpha^{106})$	$(\alpha^{8}, \alpha^{93})$
$(\alpha^{11}, \alpha^{29})$	$(\alpha^{11}, \alpha^{101})$	$(\alpha^{12}, \alpha^{81})$	$(\alpha^{12}, \alpha^{59})$
$(\alpha^{13}, \alpha^{116})$	$(\alpha^{13}, \alpha^{23})$	$(\alpha^{15}, \alpha^{63})$	$(\alpha^{15}, \alpha^{15})$
$(\alpha^{16}, \alpha^{66})$	$(\alpha^{16}, \alpha^{41})$	$(\alpha^{21}, \alpha^{13})$	$(\alpha^{21}, \alpha^{91})$
$(\alpha^{22}, \alpha^{26})$	$(\alpha^{22}, \alpha^{55})$	$(\alpha^{24}, \alpha^{86})$	$(\alpha^{24}, \alpha^{25})$
$(\alpha^{26}, \alpha^{34})$	$(\alpha^{26}, \alpha^{11})$	$(\alpha^{27}, \alpha^{96})$	$(\alpha^{27}, \alpha^{97})$
$(\alpha^{29}, \alpha^{12})$	$(\alpha^{29}, \alpha^{28})$	$(\alpha^{30}, \alpha^{6})$	$(\alpha^{30}, \alpha^{14})$
$(\alpha^{32}, \alpha^{9})$	$(\alpha^{32}, \alpha^{44})$	$(\alpha^{35}, \alpha^{107})$	$(\alpha^{35}, \alpha^{54})$
$(\alpha^{37}, \alpha^{122})$	$(\alpha^{37}, \alpha^{77})$	$(\alpha^{39}, \alpha^{94})$	$(\alpha^{39}, \alpha^{51})$
$(\alpha^{41}, \alpha^{3})$	$(\alpha^{41}, \alpha^{7})$	$(\alpha^{42}, \alpha^{58})$	$(\alpha^{42}, \alpha^{75})$
$(\alpha^{44}, \alpha^{47})$	$(\alpha^{44}, \alpha^{89})$	$(\alpha^{45}, \alpha^{64})$	$(\alpha^{45}, \alpha^{79})$
$(\alpha^{48}, \alpha^{78})$	$(\alpha^{48}, \alpha^{114})$	$(\alpha^{49}, \alpha^{68})$	$(\alpha^{49}, \alpha^{22})$
$(\alpha^{51}, \alpha^{125})$	$(\alpha^{51}, \alpha^{60})$	$(\alpha^{52}, \alpha^{43})$	$(\alpha^{52}, \alpha^{76})$
$(\alpha^{53}, \alpha^{4})$	$(\alpha^{53}, \alpha^{124})$	$(\alpha^{54}, \alpha^{17})$	$(\alpha^{54}, \alpha^{69})$
$(\alpha^{58}, \alpha^{70})$	$(\alpha^{58}, \alpha^{109})$	$(\alpha^{60}, \alpha^{39})$	$(\alpha^{60}, \alpha^{57})$
$(\alpha^{64}, \alpha^{117})$	$(\alpha^{64}, \alpha^{27})$	$(\alpha^{65}, \alpha^{72})$	$(\alpha^{65}, \alpha^{98})$
$(\alpha^{69}, \alpha^{123})$	$(\alpha^{69}, \alpha^{120})$	$(\alpha^{70}, \alpha^{40})$	$(\alpha^{70}, \alpha^{21})$
$(\alpha^{71}, \alpha^{52})$	$(\alpha^{71}, \alpha^{110})$	$(\alpha^{74}, \alpha^{18})$	$(\alpha^{74}, \alpha^{88})$
$(\alpha^{77}, \alpha^{90})$	$(\alpha^{77}, \alpha^{100})$	$(\alpha^{78}, \alpha^{83})$	$(\alpha^{78}, \alpha^{92})$
$(\alpha^{81}, \alpha^{24})$	$(\alpha^{81}, \alpha^{56})$	$(\alpha^{82}, \alpha^{126})$	$(\alpha^{82}, \alpha^{30})$
$(\alpha^{83}, \alpha^{104})$	$(\alpha^{83}, \alpha^{19})$	$(\alpha^{84}, \alpha^{80})$	$(-\alpha^{84}, \alpha^{42})$
$(\alpha^{85}, \alpha^{1})$	$(\alpha^{85}, \alpha^{31})$	$(\alpha^{86}, \alpha^{2})$	$(\alpha^{86}, \alpha^{62})$
$(\alpha^{88}, \alpha^{85})$	$(\alpha^{88}, \alpha^{38})$	$(\alpha^{89}, \alpha^{61})$	$(\alpha^{89}, \alpha^{102})$
$(\alpha^{90}, \alpha^{32})$	$(\alpha^{90}, \alpha^{103})$	$(\alpha^{96}, \alpha^{119})$	$(\alpha^{96}, \alpha^{113})$
$(\alpha^{98}, \alpha^{5})$	$(\alpha^{98}, \alpha^{82})$	$(\alpha^{99}, \alpha^{87})$	$(\alpha^{99}, \alpha^{108})$
$(\alpha^{102}, \alpha^{10})$	$(\alpha^{102}, \alpha^{37})$	$(\alpha^{104}, \alpha^{35})$	$(\alpha^{104}, \alpha^{118})$
$(\alpha^{105}, \alpha^{111})$	$(\alpha^{105}, \alpha^{99})$	$(\alpha^{106}, \alpha^{16})$	$(\alpha^{106}, \alpha^{115})$
$(\alpha^{108}, \alpha^{105})$	$(\alpha^{108}, \alpha^{46})$	$(\alpha^{120}, \alpha^{45})$	$(\alpha^{120}, \alpha^{50})$
$(\alpha^{113}, \alpha^{20})$	$(\alpha^{113}, \alpha^{74})$	$(\alpha^{116}, \alpha^{36})$	$(\alpha^{116}, \alpha^{49})$

and the zero of the group $\underline{O} = (\infty, \infty)$

† *α is a primitive root of the irreducible polynomial $f(x) = x^7 + x^3 + 1$ which generated F_{2^7} i.e* $f(\alpha) = 0$

Proof:

$$l = x^2 + x$$

$$l^{2^2} = x^{2^3} + x^{2^2}$$

$$\vdots$$

$$l^{2^{m-1}} = x^{2^m} + x^{2^{m-1}}$$

Adding we get, $\sum_{j \in J} l^{2^j} = T_2(x) + x$. Now, $T_2(x)$ is either 0 or 1 and the sum of roots equals 1.

Therefore, $x_1 = \sum_{j \in J} l^{2^j}$.

Since x_1 is a solution of Equation (3.4.6) iff $T_2(l) = 0$, $x_1 = \sum_{i \in I} l^{2^i}$.

The above theorem provides a simple and straightforward solution to Equation (3.4.6) for odd m.

Hence an overview of the procedure for finding solutions is shown in Figure 5.

Example: Consider the abelian group formed by $E : y^2 + y = x^3$ over the field $\dfrac{F_{2^7}}{(x^7 + x^3 + 1)}$. Let α be a primitive root of the polynomial. Table 3 illustrates the points on $E(F_{2^7})$ which have been simulated using the above algorithm.

Chapter 4
Elliptic Curve Cryptosystems

4.1 Elliptic Curve Cryptosystems over Finite Fields

In this section, we shall discuss the elliptic curve analogs of the various public-key cryptosystems discussed in previous chapters We start with the Elliptic Curve Pohlig-Hellman Scheme.

4.1.1 Elliptic Curve Pohlig-Hellman Scheme

Consider an elliptic curve $E(F_k)$ defined over a field F_k of characteristic $char(E(F_k))$. As discussed earlier, it forms an abelian group of order $\#E(F_k)$.

The communication is assumed to be between user A and user B. Each user M is provided a pair of keys (ϵ_M, δ_M) where ϵ_M is made public (the public-key) and δ_M is known only by user M (the private-key). If user A wishes to transmit a message $m = (x, y) \in E(F_k)$ to user B, she computes the enciphered message c as,

$$c = \epsilon_B m \tag{4.1.1}$$

where $0 < \epsilon_B < \#E(F_k)$

User B deciphers the message m by using a deciphering transformation

$$m = \delta_B c \tag{4.1.2}$$

where $0 < \delta_B < \#E(F_k)$ such that

$$\epsilon_B \delta_B \equiv 1 \pmod{\#E(F_k)} \tag{4.1.3}$$

The security of the system lies in computing the discrete logarithm problem over elliptic curve groups *i.e.*

Given an elliptic curve $E(F_p)$ defined over a field F_p, and two points $P, Q \in E(F_p)$, find an integer η such that

$$Q = \eta P \tag{4.1.4}$$

if such an η exists.

This problem seems to be more intractible than the classical discrete logarithm problem defined over multiplicative groups. The strongest techniques for the latter (like the Index Calculus method etc.) do not seem to be applicable to the elliptic curve analog. Especially in the case of F_{2^m}, the discrete logarithm over it are found to be relatively easy to compute unless m is chosen to be quite large. It is likely that the analogous system using elliptic curves over F_{2^m} will be secure with significantly smaller values of m. Hence by a careful choice of the order of the elliptic curve group by ensuring the order of the cyclic subgroups are *non-smooth* i.e. divisible by large primes only, the discrete logarithm problem can be made very difficult for the cryptanalyst.

Example: Consider elliptic curve $E : y^2 = x^3 + 1$ defined over F_{79} (see Section 3.2). This group has an order equal to 80 Let $(3, 27)$ be the pair of keys (with its usual meaning) with a user B.

Suppose A wishes to encrypt a message $m = (34, 15)$. She sends the ciphertext as $c = 3m = 3(34, 15)$. The result on simulation is $c = (57, 17)$ which is sent to B.

On receiving it B deciphers it as $m = 27c = 27(57, 17)$, which on simulation gives $m = (34, 15)$, the original messagetext.

Example: In a similar way, consider elliptic curve $E : y^2 + y = x^3 + 1$ defined over $\frac{F_{2^7}}{f(x)}$ where $f(x)$ is the irreducible polynomial $x^7 + x^3 + 1$ and let α be the primitive root $(f(\alpha) = 0)$. This group has an order equal to 129. Consider the key-pair $(5, 26)$ with user B.

Suppose A wishes to send B the message $m = (\alpha^{49}, \alpha^{68})$. She sends the encrypted text as $c = 5m = 5(\alpha^{49}, \alpha^{68}) = (\alpha^{90}, \alpha^{103})$, which is sent to B.

On receiving it B deciphers it as $m = 26c = 26(\alpha^{90}, \alpha^{103}) = (\alpha^{49}, \alpha^{68})$, which is the original messagetext

4.1.2 Elliptic Curve Massey-Omura Scheme

Consider an elliptic curve $E(F_k)$ defined over a field F_k with characteristic $char(E(F_k))$ and order $\#E(F_k)$. Here we let $F_k, E(F_k)$ and $\#E(F_k)$ to be publicly known and fixed [14].

Suppose user A wishes to communicate with user B by sending a message m. She chooses a random integer η_1 such that $0 < \eta_1 \leq \#F(F_k)$ and $gcd(\eta_1, \#E(F_k)) = 1$ and sends to B,

$$c_1 = \eta_1 m \tag{4.1.5}$$

Next B chooses a random integer ϵ_1 with the same properties and transmits to A,

$$c_2 = \epsilon_1 c_1 = \epsilon_1(\eta_1 m) \tag{4.1.6}$$

Now A chooses an integer η_2 such that $0 < \eta_2 \leq \#F(F_k)$ and $gcd(\eta_2, \#E(F_k)) = 1$ and

$$\eta_1 \eta_2 \equiv 1 \pmod{\#E(F_k)} \tag{4.1.7}$$

and sends to B,

$$\begin{aligned} c_3 &= \eta_2 c_2 \\ &= \eta_2(\epsilon_1 c_1) \\ &= \eta_2(\epsilon_1(\eta_1(m))) \\ &= \epsilon_1 m \end{aligned} \tag{4.1.8}$$

On receiving c_3, B uses an integer ϵ_2 such that $0 < \epsilon_2 \leq \#E(F_k)$ and $gcd(\epsilon_2, \#E(F_k)) = 1$ and

$$\epsilon_1 \epsilon_2 \equiv 1 \pmod{\#E(F_k)} \tag{4.1.9}$$

and decrypts the ciphertext as,

$$\begin{aligned} c_4 &= \epsilon_2 c_3 \\ &= \epsilon_2(\eta_2(\epsilon_1(\eta_1(m)))) \\ &= \epsilon_2(\epsilon_1((m))) \\ &= m \end{aligned} \tag{4.1.10}$$

Example: Consider the elliptic curve $E : y^2+y = x^3+1$ defined over F_{2^7} (See Section 3.4). Note that the order of the elliptic curve group is 129 and it is a cyclic group. Consider User A has the set of keys $(\eta_1, \eta_2) = (13, 10)$ and User B has the set of keys given by $(\epsilon_1, \epsilon_2) = (4, 97)$. Let a message $m = (\alpha^{37}, \alpha^{77})$ be encrypted by A as $c_1 = \eta_1 m = 13(\alpha^{37}, \alpha^{77}) = (\alpha^{29}, \alpha^{12})$. Next B sends back to A the ciphertext $c_2 = 4(\alpha^{29}, \alpha^{12}) = (\alpha^{96}, \alpha^{119})$. On receipt of c_2, A sends to B $c_3 = 10(\alpha^{96}, \alpha^{119}) = (\alpha^{70}, \alpha^{21})$ and B uses c_3 to get the original message $m = 97(\alpha^{70}, \alpha^{21}) = (\alpha^{37}, \alpha^{77})$. The major advantage of such a procedure is that the key-pair is totally decided by the user using it and the other communicating party need not know anything about the keys. So there is a greater flexibility for the user to change key-pairs at will. But the obvious disadvantage of such a scheme is that any pair of users have to communicate three times over a channel to broadcast a message.

4.1.3 Elliptic Curve El Gamal Scheme

Consider an elliptic curve $E(F_k)$ defined over a field F_k with characteristic $char(E(F_k))$ and order $\#E(F_k)$. Let $g \in E(F_k)$ be a fixed and publicly known point [14, 16]. Let the communication link be between user A and user B.

The receiver B chooses an integer $0 < \varphi < \#E(F_k)$ randomly and publishes the key φg keeping φ secret.

Suppose A wishes to transmit a message m to B, $m \in E(F_k)$. She chooses a random integer κ such that $0 < \kappa < \#E(F_k)$ and sends the following pair as the encrypted text to B.

$$\underline{c} = (\kappa g, m \oplus \kappa(\varphi g)) \tag{4.1.11}$$

To decrypt the message, B multiplies κg with his secret key φ and subtracts $\kappa\varphi g$ from the second point in the pair to get the original message. In actual practice, since subtraction operation is equivalent to complementary addition operation in finite fields, the decryption occurs as B uses an integer φ' satisfying $0 < \varphi' < \#E(F_k)$ and $\varphi \oplus \varphi' \equiv \underline{O} \pmod{\#E(F_k)}$ and multiplies κg with his secret key φ' and adds $\kappa\varphi' g$ to the second point in the pair to get the original message since,

$$\begin{aligned} m \oplus \kappa(\varphi g) \oplus \kappa(\varphi' g) &= m \oplus (\kappa\varphi g \oplus \kappa\varphi' g) \\ &= m \oplus \kappa g(\varphi \oplus \varphi') \\ &= m \oplus \underline{O} \\ &= m \end{aligned} \tag{4.1.12}$$

Example: Assume the elliptic curve group $E(F_{79})$ as consided above. Let the publicly known point g be $g = (56, 31)$. Suppose B chooses $\varphi = 23$ (and therefore $\varphi' = 57$ and publishes $\varphi g = 23(56, 31) = (19, 48)$. Suppose User A wishes to communicate a message $m = (11, 20)$ to B. She chooses a random $\kappa = 51$, computes $\kappa g = 51(56, 31) = (73, 47)$ and $m \oplus \kappa(\varphi g) = (11, 20) \oplus 51(19, 48) = (66, 70)$ and transmits to B the following pair of points $\big((73, 47), (66, 70)\big)$. On receiving, B computes $57(73, 47) = (5, 75)$, which when added to $(66, 70)$ gives $(11, 20)$, the message text.

Here again, the security of the system depends on the elliptic curve discrete logarithm problem.

4.2 Generalised Elliptic Curve Cryptosystem defined over Finite Rings

Till now, we have limited our discussions to cryptosystems based on finite abelian group structure. In this section, we propose to generalise this further by defining cryptosystems based on finite monoid structures. For this, let us first consider a ring Z_n where n is a product of large primes $\{p_i\}$ $\quad \forall i \in \{0, 1, \cdots, k-1\}$ *i.e.*

$$n = \prod_{i=0}^{k-1} p_i \tag{4.2.1}$$

Now, the ring Z_n can be decomposed as a direct sum of rings as

$$Z_n \cong Z_{p_0} \bigoplus Z_{p_1} \bigoplus \cdots \bigoplus Z_{p_{k-1}} \tag{4.2.2.a}$$

or equivalently,

$$Z_n \cong \bigoplus_{i=0}^{k-1} Z_i \tag{4.2.2.b}$$

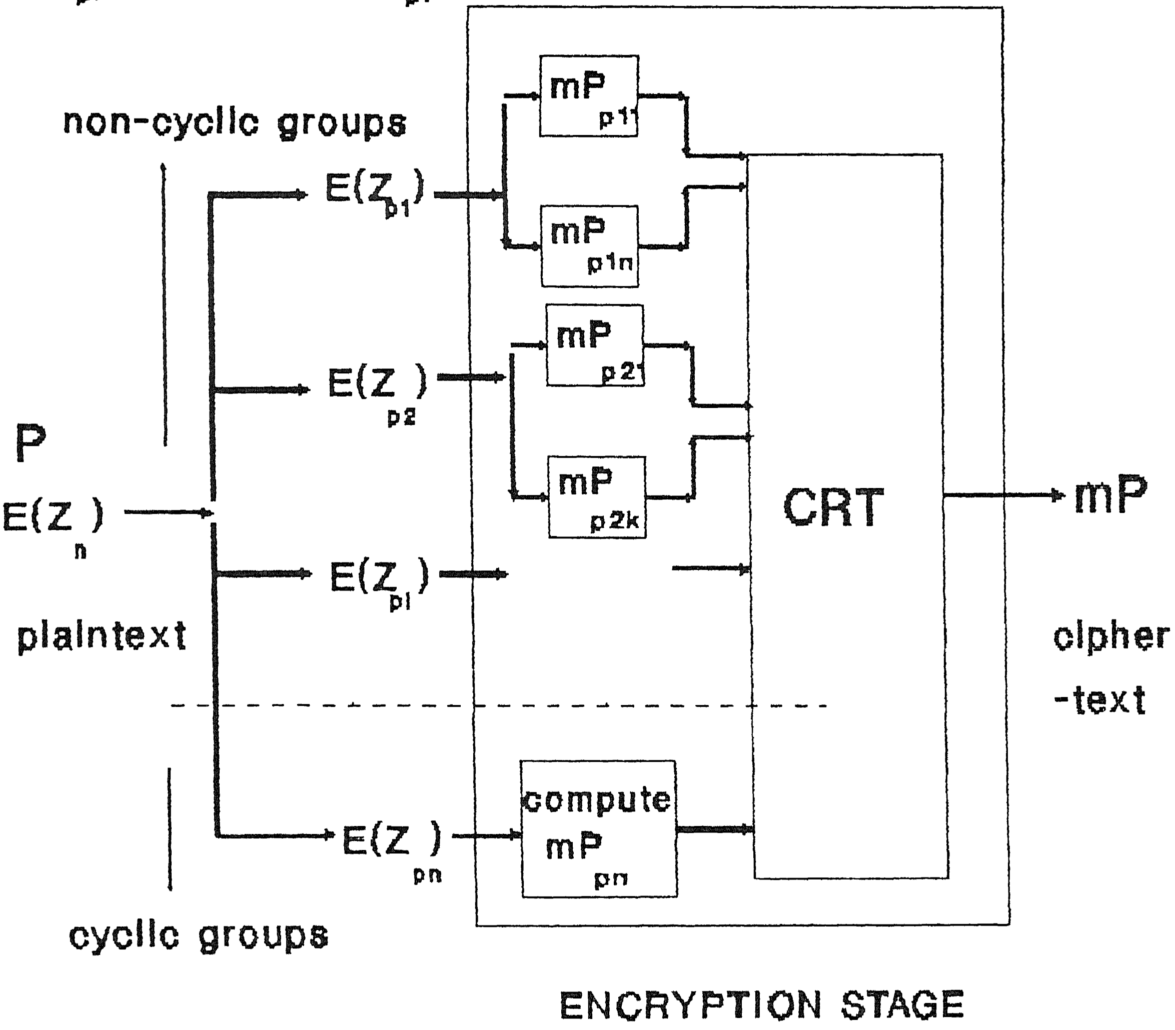
Consider an elliptic curve E defined over the above ring Z_n and represented as $E(Z_n)$. Now, we find that the structure formed by $E(Z_n)$ is, in general, a monoid structure (we shall soon find out that there are certain points on the elliptic curve structure which do not have well-defined group operation). Obviously, there are certain difficulties when we define cryptosystems over such a monoid structure since there may be certain messages which we

FIGURE 6:

GENERALISED CRYPTOGRAPHIC SYSTEM

P and mP belong to $E(Z_n)$

P_{pi} belongs to $E(Z_{pi})$



may not be able to recover after they are encrypted. This is because in an abelian group structure, we are guaranteed to recover message from ciphertext because each element of the group has a well-defined unique inverse. Hence, there is a finite probability of error that we would not be able to recover our message text after it is encrypted in such a scheme.

To carry out encryption and decryption schemes, we use the following procedure. Since the elliptic curve monoid $E(Z_n)$ can be further decomposed as

$$E(Z_n) \cong E(Z_{p_0}) \bigoplus E(Z_{p_1}) \bigoplus \cdots \bigoplus E(Z_{p_{k-1}}) \tag{4.2.3.a}$$

or equivalently,

$$E(Z_n) \cong \bigoplus_{i=0}^{k-1} E(Z_{p_i}) \tag{4.2.3.b}$$

Now, each of the $E(Z_{p_i})$ $\forall i \in \{0, 1, \cdots k-1\}$ are abelian group structures which may or may not be cyclic groups. In case they are non-cyclic groups, they can be further decomposed as a direct sum of cyclic subgroups *i.e.*

$$\begin{aligned} E(Z_n) &\cong \bigoplus_{j\in J} \underbrace{E(Z_{p_j})}_{cyclic} \bigoplus_{j\in K} \underbrace{E(Z_{p_j})}_{non-cyclic} \\ &\cong \bigoplus_{j\in J} \underbrace{E(Z_{p_j})}_{cyclic} \bigoplus_{j\in K} \underbrace{(\bigoplus_{m\in L} E(Z_{p_{j_m}}))}_{cyclic} \end{aligned} \tag{4.2.4}$$

where J is the set of all cyclic subgroups of $E(Z_n)$, K is the set of non-cyclic subgroups of $E(Z_n)$ and L is the set of all cyclic subgroups of set K. Figure 6 illustrates the above statement.

Consider a point $P \in E(Z_n)$ to be encrypted as $Q = \eta P$ where $Q \in E(Z_n)$ and $\eta \in Z$, the set of positive integers. We can carry out the above operation by first decomposing P as

$$P \cong \bigoplus_{i=0}^{k-1} P_{p_i} \tag{4.2.5}$$

Table 4: Monoid Structure formed by Elliptic Curve E $y^2 = x^3 + 1$ over the Ring Z_{55}

(0 , 1)	(0 , 54)
(0 , 21)	(0 , 34)
(2 , 3)	(2 , 52)
(2 , 8)	(2 , 47)
(5 , 4)	(5 , 51)
(5 , 26)	(5 , 29)
(7 , 17)	(7 , 38)
(7 , 27)	(7 , 28)
(9 , 20)	(9 , 35)
(10 , 11)	(10 , 44)
(20 , 9)	(20 , 46)
(20 , 24)	(20 , 31)
(22 , 12)	(22 , 43)
(22 , 23)	(22 , 32)
(24 , 25)	(24 , 30)
(27 , 7)	(27 , 48)
(27 , 18)	(27 , 37)
(29 , 5)	(29 , 50)
(32 , 22)	(32 , 33)
(35 , 14)	(35 , 41)
(35 , 19)	(35 , 36)
(40 , 6)	(40 , 49)
(40 , 16)	(40 , 39)
(42 , 13)	(42 , 42)
(43 , 2)	(43 , 53)
(44 , 10)	(44 , 45)
(49 , 15)	(49 , 40)
(50 , 0)	(∞ , ∞)

and points notionally represented as $(\aleph_1)$, $(\aleph_2)$, , $(\aleph_{15})$ † which are also elements of the monoid structure

† *see Table 5*

Table 5: Decomposing Monoid $E(Z_{55})$ using $E(Z_{55}) \cong E(Z_5) \bigoplus E(Z_{11})$, a direct sum of two Abelian Groups

(0, 1)	$\cong$	(0, 1)	$\bigoplus$	(0, 1)	(0, 54)	$\cong$	(0, 4)	$\bigoplus$	(0, 10)
(2, 3)	$\cong$	(2, 3)	$\bigoplus$	(2, 3)	(2, 52)	$\cong$	(2, 2)	$\bigoplus$	(2, 8)
(5, 4)	$\cong$	(0, 4)	$\bigoplus$	(5, 4)	(5, 51)	$\cong$	(0, 1)	$\bigoplus$	(5, 7)
(7, 17)	$\cong$	(2, 2)	$\bigoplus$	(7, 6)	(7, 38)	$\cong$	(2, 3)	$\bigoplus$	(7, 5)
(9, 20)	$\cong$	(4, 0)	$\bigoplus$	(9, 9)	(9, 35)	$\cong$	(4, 0)	$\bigoplus$	(9, 2)
(10,11)	$\cong$	(0, 1)	$\bigoplus$	(10, 0)	(10,44)	$\cong$	(0, 4)	$\bigoplus$	(10, 0)
(20, 9)	$\cong$	(0, 4)	$\bigoplus$	(9, 9)	(20,46)	$\cong$	(0, 1)	$\bigoplus$	(9, 2)
(22,12)	$\cong$	(2, 2)	$\bigoplus$	(0, 1)	(22,43)	$\cong$	(2, 3)	$\bigoplus$	(0, 10)
(24,25)	$\cong$	(4, 0)	$\bigoplus$	(2, 3)	(24,30)	$\cong$	(4, 0)	$\bigoplus$	(2, 8)
(27, 7)	$\cong$	(2, 2)	$\bigoplus$	(5, 7)	(27,48)	$\cong$	(2, 3)	$\bigoplus$	(5, 4)
(29, 5)	$\cong$	(4, 0)	$\bigoplus$	(7, 5)	(29,50)	$\cong$	(4, 0)	$\bigoplus$	(7, 6)
(32,22)	$\cong$	(2, 2)	$\bigoplus$	(10, 0)	(32,33)	$\cong$	(2, 3)	$\bigoplus$	(10, 0)
(35,14)	$\cong$	(0, 4)	$\bigoplus$	(2, 3)	(35,41)	$\cong$	(0, 1)	$\bigoplus$	(2, 8)
(40, 6)	$\cong$	(0, 1)	$\bigoplus$	(7, 6)	(40,49)	$\cong$	(0, 4)	$\bigoplus$	(7, 5)
(42, 2)	$\cong$	(2, 2)	$\bigoplus$	(9, 2)	(42,53)	$\cong$	(2, 3)	$\bigoplus$	(9, 9)
(44,10)	$\cong$	(4, 0)	$\bigoplus$	(0, 10)	(44,45)	$\cong$	(4, 5)	$\bigoplus$	(0, 1)
(49,15)	$\cong$	(4, 0)	$\bigoplus$	(5, 4)	(49,40)	$\cong$	(4, 0)	$\bigoplus$	(5, 7)
(54, 0)	$\cong$	(4, 0)	$\bigoplus$	(10, 0)	(54, 0)	$\cong$	(4, 0)	$\bigoplus$	$(10, 0^{\dagger})$
$(\aleph_1 \quad)$	$\cong$	(0, 1)	$\bigoplus$	(∞,∞)	$(\aleph_2 \quad)$	$\cong$	(0, 4)	$\bigoplus$	(∞,∞)
$(\aleph_2 \quad)$	$\cong$	(2, 2)	$\bigoplus$	(∞,∞)	$(\aleph_3 \quad)$	$\cong$	(2, 3)	$\bigoplus$	(∞,∞)
$(\aleph_4 \quad)$	$\cong$	(∞,∞)	$\bigoplus$	(0, 1)	$(\aleph_5 \quad)$	$\cong$	(∞,∞)	$\bigoplus$	(0, 10)
$(\aleph_6 \quad)$	$\cong$	(∞,∞)	$\bigoplus$	(2, 3)	$(\aleph_7 \quad)$	$\cong$	(∞,∞)	$\bigoplus$	(2, 8)
$(\aleph_8 \quad)$	$\cong$	(∞,∞)	$\bigoplus$	(5, 4)	$(\aleph_9 \quad)$	$\cong$	(∞,∞)	$\bigoplus$	(5, 7)
$(\aleph_{10} \quad)$	$\cong$	(∞,∞)	$\bigoplus$	(7, 5)	$(\aleph_{11} \quad)$	$\cong$	(∞,∞)	$\bigoplus$	(7, 6)
$(\aleph_{12} \quad)$	$\cong$	(∞,∞)	$\bigoplus$	(9, 2)	$(\aleph_{13} \quad)$	$\cong$	(∞,∞)	$\bigoplus$	(9, 9)
$(\aleph_{14} \quad)$	$\cong$	(∞,∞)	$\bigoplus$	(10, 0)	$(\aleph_{15}^{\ddagger} \quad)$	$\cong$	(∞,∞)	$\bigoplus$	(10, 0)

$\dagger$ · point 1 of order 2

$\ddagger$ · point 2 of order 2

where $P_{p_i} \in E(Z_{p_i}) \forall i \in \{0, 1, \cdots, k-1\}$. Now, we have a well-defined addition operation defined over $E(Z_{p_i}) \forall i \in \{0, 1, \ldots, k-1\}$. Hence, $Q = \eta P$ can be computed as,

$$Q_{p_i} = \eta P_{p_i} \tag{4.2.6}$$

$\forall i \in \{0, 1, \cdots, k-1\}$. We may further decouple the addition operation by considering operations over non-cyclic groups as addition operations over their cyclic subgroups. So, in general, we have the following sets of equations governing the above addition operation,

$$\begin{aligned} Q_{p_j} &= \eta P_{p_j} \qquad (4.2.7) \\ Q_{p_{j_m}} &= \eta P_{p_{j_m}} \end{aligned}$$

where $j \in J$, $j_m \in L$ as defined above. To get back Q from the various Q_{p_k} where $k \in J \cup L$, we use the Chinese Remainder Theorem.

Theorem 4.2.1. *(Chinese Remainder Theorem) Let $m_0, m_1, \cdots, m_n \in Z$ be integers which are pairwise relatively prime, i.e $gcd(m_i, m_j) = 1$ for $i \neq j$ and let $u_i \in Z_{m_i}, i \in \{0, 1, \cdots, n\}$ be $n+1$ specified residues. For any fixed integer $a \in Z$, there exists a unique integer $u \in Z$ which satisfies the following conditions*

$$\begin{aligned} a \leq u \leq a + m, &\qquad \text{where } m = \prod_{i=0}^{n} m_i \qquad (4.2.8) \\ u \equiv u_i \pmod{m_i}&, 0 \leq i \leq n \end{aligned}$$

In particular, it has a unique solution $x \in Z_m$. The value of x is given by $x = u_1 m y_1 + u_2 m y_2 + \cdots + u_n m y_n$ where $m_i' y_i \equiv 1 \pmod{m_i}, i \in \{0, 1, \cdots, n\}$ and $m_i' = \dfrac{m}{m_i}, i \in \{0, 1, \cdots, n\}$.

Hence, we are able to encrypt a message $m = P \in E(Z_n)$ as $c = \eta P \in E(Z_n)$. Decryption of m from c can be done as

$$m = \eta' c \tag{4.2.9}$$

where $\eta' \in Z$ such that

$$\eta\eta' \equiv 1 \pmod{\# m} \tag{4.2.10}$$

where $\#m = lcm(\#E(Z_{p_0}), \#E(Z_{p_1}), \cdots, \#E(Z_{p_{k-1}}))$, $\#E(Z_{p_i})$ is the order of the abelian group $E(Z_{p_i}) \forall i \in \{0, 1, \cdots, k-1\}$. We use a procedure similar to the one outlined above (replace η' for η) to recover m.

However, there are a few ciphers $(\aleph_i) \in \Pi$ where $i \in \{0, 1, \cdots, p\}$ where $p \in Z$ from which we are unable to recover the original messages after decryption. We shall derive a closed form expression for the probability of error after illustrating with an example.

Example: Consider the ring Z_{55} and an elliptic curve $E : y^2 = x^3 + 1$ defined over it. We denote it by $E(Z_{55})$ which forms a monoid structure. The points in the elliptic curve monoid are given in Table 4. Note that there are points $(\aleph_i), i \in \{0, 1, \cdots, 15\}$ for which the group addition law is not well-defined. Table 5 illustrates the decomposition, $E(Z_{55}) \cong E(Z_5) \bigoplus E(Z_{11})$, which are finite abelian group (in fact cyclic as well). The order of these groups are 6 and 12 (See Chapter 3) respectively.

Consider a point $P = (7, 38) \in E(Z_{55})$ which is to be encrypted as $Q = 5P = 5(7, 38)$. Using the fact,

$$(7, 38) \cong (2, 3) \bigoplus (7, 5) \tag{4.2.11}$$

and thus,

$$5(7, 38) \cong 5(2, 3) \bigoplus 5(7, 5) \tag{4.2.12}$$

which on computation is $(5, 4) \bigoplus (4, 0)$. To calculate the point $Q \in E(Z_{55})$, we use the CRT as,

determine $(x, y) \in E(Z_{55})$, such that $(x, y) \cong (5, 4) \bigoplus (4, 0)$. The set of equations are

$$\begin{aligned} x &\equiv 5 \pmod{11} \qquad & x &\equiv 4 \pmod{5} \\ y &\equiv 4 \pmod{11} \qquad & y &\equiv 0 \pmod{5} \end{aligned} \tag{4.2.13}$$

$\{m_1, m_2, y_1, y_2\} = \{5, 11, 9, 1\}$ from which we obtain $(x, y) = (49, 15)$, the desired solution.

It can be noted from the example that the set of ciphers $(\aleph_i) \in \Pi, i \in \{0, 1, \cdots, k-1\}$ have at least one tuple equal to (∞, ∞) when represented in k-tuple form. Hence, all the ciphers N which can be recovered is given by

$$N = (\#E(Z_{p_0}) - 1)(\#E(Z_{p_1}) - 1) \cdots (\#E(Z_{p_{k-1}}) - 1) \tag{4.2.14}$$

Table 6 *: List of exponentials for which $\frac{2^m+1}{3}$ is Prime

Exponent power range	*Exponents*
2 – 100	3, 5, 7, 11, 17, 19, 23, 31, 41, 43, 47, 53, 59, 61, 71, 79, 83, 89
100 – 200	101, 107, 113, 127, 131, 137, 149, 167, 173, 179, 191, 197, 199
200 – 300	227, 233, 239, 251, 257, 263, 269, 281, 293
300 – 400	311, 313, 317, 341, 347, 353, 359, 383, 389
400 – 500	401, 419, 431, 443, 449, 461, 467, 479, 491
500 – 600	503, 509, 521, 557, 563, 569, 587, 593 †, 599
600 – 700	617, 641, 647, 653, 659, 677, 683
700 – 800	701, 719, 743, 761, 773, 797
800 – 900	809, 821, 827, 839, 857, 863, 881, 887

* *Reproduced from Bender and Castagloni [2]*

† *Maximum value of cryptosystem implementation reported so far*

and the total number of points on $E(Z_n)$ given by S is

$$S = (\#E(Z_{p_0}))(\#E(Z_{p_1}))\cdots(\#E(Z_{p_{k-1}})) \tag{4.2.15}$$

Hence the *probability of error* given by $Pr(E(Z_n))$ is

$$\begin{aligned} Pr(E(Z_n)) &= 1 - \frac{N}{S} \\ &= 1 - \frac{(\#E(Z_{p_0}) - 1)(\#E(Z_{p_1}) - 1)\cdots(\#E(Z_{p_{k-1}}) - 1)}{(\#E(Z_{p_0}))(\#E(Z_{p_1}))\cdots(\#E(Z_{p_{k-1}}))} \\ &\approx \frac{1}{\#E(Z_{p_0})} + \frac{1}{\#E(Z_{p_1})} + \cdots + \frac{1}{\#E(Z_{p_{k-1}})} \end{aligned} \tag{4.2.16}$$

since the order of the subgroups are assumed to be very large. For example, in a typical case, if the minimum order of the subgroups is around 100 decimal digits, then probability of error $\approx 10^{-100}$ which is very small and can be tolerated for practical purposes.

4.3 Security Aspects

In this section, we discuss some basic requirements for a safe elliptic curve cryptosystem.

4.3.1 Non b-smooth Orders

There exists no subexponential algorithms for solving the discrete logarithm problem on a general elliptic curve; the fastest known techniques [2, 4, 13, 15] over multiplicative groups do not seem to be effective on elliptic curve groups. The general algorithm "Baby-Step Giant-Step " algorithm (which applies to any group) requires time fully exponential in the length of the largest prime factor of the order of the group. Hence, in order to avoid an easy solution to the discrete logarithm problem, it is important to search for elliptic curves with orders of its cyclic subgroups being non b-smooth numbers (defined below).

Definition: [21] Let b be a positive integer. A number m is said to be b-smooth is every prime factor q of m is less than or equal to b. Thus,

$$m = \prod_{e_q \leq b} (q_{e_q}) \tag{4.3.1}$$

Numbers which are b-smooth are rare. The probability that a random number $m \leq x$ is b-smooth is about u^{-u} where $u = \frac{log x}{log b}$. (example: if $x = 10^{100}, b = 10^{10}$, then $u = 10$ and probability $= 10^{-10}$).

A choice of large factors (see Table 6) is recommended for constructing elliptic curve groups for cryptosystems.

4.3.2 Non-Singular Elliptic Curves

Consider elliptic curve $E(F_k)$ defined by the general Weirstrass equation over a field F_k. Consider a point $P = (x_1, y_1) \in E(F_k)$ which is the only singularity in $E(F_k)$. With a change of variables as

$$x \longrightarrow x' + x_1 \qquad (4.3.2)$$

$$y \longrightarrow y' + y_1$$

we assume that Weirstrass equation reduces to

$$E : y^2 + a_1xy - a_2x^2 - x^3 = 0 \qquad (4.3.3)$$

where $a_1, a_2 \in F_k$ with singular point $P = (0,0)$. Let

$$y^2 + a_1xy - a_2x^2 = (y - \alpha x)(y - \beta x) \qquad (4.3.4)$$

where $\alpha, \beta \in F_k$ or F_{k_1} (defined as the quadratic extension of F_k). Then P is called a node if $\alpha \neq \beta$, and a cusp if $\alpha = \beta$. Let $E_{ns}(F_k)$ denote the set of solutions $(x, y) \in F_k \times F_k$ to Equation (4 3.3), excluding the point P and including the point at infinity, $\underline{O}$. $E_{ns}(F_k)$ is called the non-singular part of $E(F_k)$. The group operation, addition, over this set follows the standard chord-and-tangent law. The following theorems [2] illustrate isomorphic relations with F_k^+, the additive group of F_k, and F_k^*, the multiplicative group of non-zero elements of F_k

Theorem 4.3.1 *i) If P is a node, and $\alpha, \beta \in F_k$, then the map $\phi : E_{ns}(F_k) \longrightarrow F_k$, defined by*

$$\phi : \underline{O} \longrightarrow 1 \qquad (4.3.5)$$

$$\phi : (x, y) \longrightarrow \left(\frac{y - \beta x}{y - \alpha x}\right)$$

is a group isomorphism.

ii) If P is a node, and $\alpha, \beta \notin F_k$, $\alpha, \beta \in F_{k_1}$, let N be the subgroup of $F_{k_1}^*$ consisting of elements of norm 1 (namely, the primitive roots of 1 in the extension field F_{k_1}). The map $\psi : E_{ns}(F_k) \longrightarrow N$ defined by

$$\psi : \underline{O} \longrightarrow 1 \qquad (4.3.6.a)$$
$$\psi : (x, y) \longrightarrow \left(\frac{y - \beta x}{y - \alpha x}\right)$$

is a group isomorphism.

iii) If P is a cusp, then the map $\omega : E_{ns}(F_k) \longrightarrow F_k^+$ defined by

$$\omega : \underline{O} \longrightarrow 0 \qquad (4.3.6.b)$$
$$\omega : (x, y) \longrightarrow \left(\frac{x}{y - \alpha x}\right)$$

is a group isomorphism.

Theorem 4.3.2 *Let $E(F_k)$ be a singular elliptic curve defined over F_k with singular point P.*

i) If P is a node, then the logarithm problem of $E_{ns}(F_k)$ is reducible in polynomial time to the logarithm problem in F_k or F_{k_1}, depending on whether $\alpha \in F_k$ or $\alpha \notin F_k$ respectively.

ii) If P is a cusp, then the logarithm problem of $E_{ns}(F_k)$ is reducible in polynomial time to the logarithm problem in F_k^+.

Now, the logarithm problem in F_k^+ can be efficiently solved in polynomial time and thus by the above isomorphic relations, the problem of discrete logarithms in elliptic curve groups can also be solved in polynomial time. Hence, selecting an elliptic curve with singularities offer no advantage over finite fields for the implementation of cryptographic protocols whose security is based on the difficulty of computing discrete logarithms in a group Instead, there is a major drawback that the group operation in $E_{ns}(F_k)$ is more computationally more intensive than group operations in the field F_k.

4.4.3 Homomorphic and Isomorphic Attacks

4.4.3.1 Homomorphic Attacks

The encryption and decryption functions $\Gamma(.)$ and $\Upsilon(.)$ observe homomorphic property for group addition operation,

$$\begin{aligned}\Gamma(m_1 \oplus m_2) &= \Gamma(m_1) \oplus \Gamma(m_2) \\ \Upsilon(m_1 \oplus m_2) &= \Upsilon(m_1) \oplus \Upsilon(m_2)\end{aligned} \qquad (4.4.7)$$

for two points m_1 and m_2 on the same elliptic curve $F(F_k)$. This is because the functions $\Gamma(.)$ and $\Upsilon(.)$ have the form

$$\begin{aligned}\Gamma : c &= \eta m \\ \Upsilon : m &= \varphi c\end{aligned} \qquad (4.4.8)$$

where $c, m \in E(F_k)$ and $\eta, \varphi \in Z$ and thus due to this linear relationship, the above homomorphic property is observed. This becomes a case for cryptanalytic attack as any cryptanalyst who knows the message-ciphertext relation for two messages m_1 and m_2 also knows the ciphertext for the valid message $(m_1 \oplus m_2)$. Obviously, by knowing more pairs, the cryptanalyst gets to know a wider range of ciphertexts [8].

To counterattack such an attack, we could either have an elliptic curve group of very large order in which all the points of the group do not constitute valid messages (with the prior mutual consent of the two parties communicating) and thus try to reduce chances of such homomorphic attacks. However, this is at the cost of low information rate. A second procedure could be to have the encryption function of the form

$$\Gamma' : c = \eta m \oplus k \qquad (4.4.9)$$

where k is any arbitrary point $\in E(F_k)$ agreed by both the parties. Here, a homomorphic attack is not possible since,

$$\Gamma'(m_1 \oplus m_2) \neq \Gamma'(m_1) \oplus \Gamma'(m_2) \qquad (4.4.10)$$

The receiver decrypts by first subtracting point k from received ciphertext and then follow the standard procedure for decryption. Hence, the cost incurred here is the additional computations at the sender and the receiver ends.

Example: Consider elliptic curve $E: y^2 = x^3 + 1$ over F_{79} (see Example above in Section 3 1) and message text and keys as previously stated Assume k to be the point (11, 59) on $E(F_{79})$, then $c = 38m \oplus k = 38(34, 15) \oplus (11, 59)$, which is found to be $c = (58, 14)$ which is transmitted to B.

Now, B decrypts the cipher by first *subtracting* k from c as $m' = (58, 14) \oplus (58, 65) = (57, 17)$, and then following the usual procedure for decryption *i.e* $m = 42m' = 42(57, 17) = (34, 15)$, the original messagetext.

Here, at both the sender and receiver ends, we incur extra computation namely, adding to and *subtracting* k from the ciphertext. However, it guarantees us security from homomorphic attacks, since the problem is as hard as finding the order of the abelian group over which the cryptosystem is based on.

4.3.3.2 Isomorphic Attacks

As stated in Theorem 3.1.2, two elliptic curves defined over a field F_k are isomorphic if the relation stated holds true So a method of cryptanalytic attack would be to identify one such isomorphic relation between the actual elliptic curve group over which the cryptosystem is based upon and another elliptic curve group used by the cryptanalyst. Therefore, by the unique one-to-one correspondence depending on the value u, the cryptanalyst can determine all points on the original elliptic curve group by determining all the points on the second elliptic curve group. However, this scheme is very difficult since it is found that the probability that there exists a u satisfying the isomorphic relation as stated above is negligibly small $\left(\propto \frac{1}{\#E(F_k)}\right)$ for large orders of the group $E(F_k)$. Also, in a practical implementation scheme, the elliptic curve group is changed (discussed later) from time to time, making such attacks even more difficult.

Chapter 5
Some Computational Aspects

In this chapter, we shall refer to some important computational issues involved in the implementation of elliptic curve cryptosystems.

5.1 Using Affine and Projective Coordinate System

Let us briefly discuss a few facts from algebraic geometry [2, 6, 16].

5.1.1 Homogeneous Polynomial

Suppose $f(x_1, x_2, \cdots, x_n) \in K(x_1, x_2, \cdots, x_n)$ be a homogeneous polynomial of degree m, i.e

$$f(tx_1, tx_2, \cdots, tx_n) = t^n f(x_1, x_2, \cdots, x_n) \tag{5.1.1}$$

A point $(a_1, a_2, \cdot\cdot, a_n) \in K^n$ satisfies

$$f(x_1, x_2, \cdots, x_n) = 0 \tag{5.1.2}$$

if and only if $(ta_1, ta_2, \cdot\cdot\ , ta_n)$ does for all $t \in K^*$ (K^* is the multiplicative group of the elements of K) $\underline{0} = (0, 0, \cdot\cdot\ 0)$ always satisfies Equation (5 1 1) and is called its trivial solution. This leads to the concept of projective space.

5.1.2 Projective and Affine Spaces

For any field K, let

$$K^n = \{(x_1, x_2, \cdot\ \cdot, x_n) \mid x_j \in K, j = 1, 2, \cdots, n\} \tag{5.1.3}$$

be a vector space of n-tuples of elements of K. On the set

$$K^{n+1} - \{\underline{0}\} = \{\underline{x} \in K^{n+1} \mid \underline{x} \neq \underline{0}\} \tag{5.1.4}$$

define an equivalence relation by $\underline{x} \sim \underline{y}$ if and only if $\underline{y} = t\underline{x}$ for some $t \in K^*$. Then the set

$$P^n(K) = K^{n+1} - \{\underline{0}\} \tag{5.1.5}$$

of equivalence classes is called the projective space over K, i.e. $P^n(K)$ consists of all nonzero vectors in K^{n+1} with two vectors $\underline{x}, \underline{y}$ not considered different if $\underline{y} = t\underline{x}$ with $t \in K^*$. We can also think of $P^n(K)$ as consisting of lines through the origin $\underline{0}$ of K^{n+1}. The affine space $A^n(K)$ may be regarded a subset of $P^n(K)$ by the map

$$A^n(K) \ni *(x_1, x_2, \cdots, x_n) \longrightarrow (x_1, x_2, \cdots, x_n, 1) \in P^n(K) \qquad (5.1.6)$$

5.1.3 Plane Algebraic Curves

A curve C defined over a field K is the set of solutions in $K \times K$ of the polynomial equation

$$C : f(x, y) = 0 \qquad (5.1.7)$$

A projective curve L over K is the set of solutions in $P^2(K)$ of the homogeneous equation

$$L : F(X, Y, Z) = 0 \qquad (5.1.8)$$

with $F(X, Y, Z) \in K(X, Y, Z)$. One can homogenise Equation (5.1 7) to get Equation (5 1 8) by putting $x = \frac{X}{Z}, y = \frac{Y}{Z}$ and then multiplying throughout by $Z^{deg(f)}$ Suppose (5 1 8) is obtained from (5 1.7) as above. Then it is a projective model for the affine curve C as defined by the former The solutions for C are precisely those solutions of L for which $Z \neq 0$, because (a, b) is a point on C if and only if $(a, b, 1)$ is a point in L. The point (a, b, c) on L with $c = 0$ is called the point of infinity on C The line of infinity is the set of all points (X, Y, Z) in $P^2(K)$ for which $Z = 0$. The points on (5.1.7) are called the affine part of the projective curve (5 1.8). A projective curve is complete in the sense that it has the points at infinity that are missing from its affine part.

5.1.4 Singularities of a Curve

Let L be a projective curve as (5 1 8) We say L is of order n if $deg(F) = n$. A point P on L is called a multiple point of multiplicity $r \geq 1$ or an r-fold point if all the partial derivatives of $F(X, Y, Z)$ of order $< r$ vanish at P, but there is a partial derivative of order r that does not vanish at P If $r = 1$, P is called a regular or non-singular point, if $r > 1$,

P s called a singular point, e g. for $r = 2$, it is called a double point and so on. A curve is singular if it has a singularity, otherwise it is non-singular or smooth.

Example: Let C be the affine curve $y^2 = x^3$.

To homogenise the equation, put $x = \frac{X}{Z}, y = \frac{Y}{Z}$.

$$F(X,Y,Z) = Y^2Z - X^3 = 0 \tag{5.1.9}$$

Singularities must satisfy

$$\begin{aligned} \frac{\partial F}{\partial X} &= -3X^2 = 0 \\ \frac{\partial F}{\partial Y} &= 2YZ = 0 \\ \frac{\partial F}{\partial Z} &= Y^2 = 0 \end{aligned} \tag{5.1.10}$$

which are of the form $(0,0,Z)$ such that $Z \neq 0$. Thus $(0,0,1)$ is the only singularity of C. It is a double point, since $\frac{\partial^2 F}{\partial Y^2}|_P \neq 0$.

Coming back to the general Weirstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.1.1}$$

where $\{a_i\} \in K$ and $(x,y) \in K \times K$.

Homogenising this equation to get the projective curve equivalent,

Put $x = \frac{X}{Z}, y = \frac{Y}{Z}$ to get an equation of degree 3

$$Y^2Z + a_1XYZ + a_3YZ^2 = x^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{5.1.11}$$

Here the projective plane $P^2(K)$ over K is the set of equivalence classes of the relation $\sim$ acting on the set

$$K^3 - \{\underline{0}\} \tag{5.1.12}$$

where $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ if and only if there exists a $u \in K^*$ such that $x_1 = ux_2, y_1 = uy_2, z_1 = uz_2$ We denote the equivalence class containing (x,y,z) by $(x : y : z)$.

The equation is said to be smooth or non-singular if all the projective points $P = (X : Y : Z) \in P^2(K)$ satisfying

$$L : F(X, Y, Z) \tag{5.1.8}$$

we get $\left(\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}, \frac{\partial F}{\partial Z}\right)\Big|_P \neq (0,0,0)$.

If all the three partial derivatives vanish at P, then P is called a singular point. There is exactly one point in E with z-coordinate equal to 0, namely $(0 : 1 : 0)$. We call this point at infinity and denote by $\underline{Q}$. Thus an elliptic curve E is the set of solutions to Equation (3.1.1) $\in K \times K$ together with the extra point at infinity $\underline{O}$.

5.1.5 Addition Formula using Projective Coordinate System

We consider two cases, a) the case for F_k where $char(F_k) > 3$ and b) the case for $F_k, k = 2^m$, $char(F_k) = 2$.

a) Case for F_k where $char(F_k) > 3$

Recalling the addition formula, given $P = (x_1, y_1) \in E$ and $Q = (x_2, y_2) \in E$, then $P \oplus Q = (x_3, y_3)$ where

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned} \tag{3.2.9}$$

where

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1}, & \text{if } P = Q \end{cases} \tag{3.2.10}$$

In projective coordinates,

$$\begin{aligned} P &= (x_1 \cdot y_1 : 1) \\ Q &= (x_2 \quad y_2 \cdot z_2) = \left(\frac{x_2}{z_2} : \frac{y_2}{z_2} : 1\right) \end{aligned} \tag{5.1.13}$$

To find $R = (x_3 \cdot y_3 \quad 1)$,

Computation time comparison for Affine and Projective Coordinate Systems

Table 7.a: $E: y^2 = x^3 + x + 1$ over $F_{4653127}$, point (653213, 1459237)

Repetitions	Affine System (in sec)	Projective System (in sec)
1631	0 097088	0 097920
2013	0 136640	0 136032 †
5381	0 195584	0.194688
12963	0 632192	0 616256
53319	2 821888	2.340128
109493	4 986368	3 204416
605503	25.000640	17 844864
933815	46 786368	29 417280
2341651	115 691392	59 172800

Table 7.b: $E \cdot y^2 + y = x^3 + x + 1$ over $\frac{F_{2^{17}}}{x^{17} + x^3 + 1}$, point $(\alpha^{787}, \alpha^{58941})$

Repetitions	Affine System (in sec)	Projective System (in sec)
301	0 440128	0 458400
417	0 532192	0.502364 †
863	0 952480	0.791888
2057	2.86576	1 827104
4573	5 019200	3.478400
113931	10.271104	6.616256

† *beyond this, projective system is computationally faster than affine system.*

$$x_3 = \frac{3x_1A'B' - A'^3z_1 - y_1B'^3z_1}{z_3} \qquad (5.1.19)$$
$$y_3 = \frac{B'(A'^2 - 2B'^3x_1)}{z_3}$$

One of the major problems using affine (non-homogeneous) equations is that repeated division is required at each stage. Now using projective coordinate system, at each step we compute the three-tuple (x_3, y_3, z_3) and perform the next operation using the same three-tuple and at the final step perform the inversion by factor z_3. Thus we reduce the computation time by performing the time-consuming inversion operation only in the final step.

As an example of encryption (or similarly in decryption) stage, consider a message $m = P$ to be enciphered as $Q = \eta P$ where $\eta \in Z$. Now if P is the affine point $(x_1, y_1, 1)$, we compute ηP by adding P to itself and then adding this result to P and so on keeping the three-tuple result (x_3, y_3, z_3) at each stage and adding it to $(x_1, y_1, 1)$ at the next stage. Finally the result (x_3, y_3, z_3) can be converted back into affine coordinated by dividing each coordinate by z_3.

The method is especially useful when large number of additions are required. As a practical example arithmetic in $F_{2^{155}}$ has been reported where multiplication of two elements take 1300 clock cycles with inversion $50,000$ cycles at a clock rate of 20 MHz. Thus at each step we save by not having to perform a costly inversion. However, the trade-off incurred is that this computation time gain is at the expense of extra register storage elements. This trade-off is apparant for lower values of repetitions as shown in Table 7.

Example: For the elliptic curve group $E : y^2 = x^3 + x + 1$ over $F_{4531217}$ and a point $(653213, 1459237)$ which belongs to the group, simulation was done (in C language source code) to compare the computation times for affine and projective coordinate systems for various values of repetitions. It is observed from the table that for lower values of repetitions, affine system of representation is computationally faster. This is because of the additional computation required for the third coordinate offsets the advantage of fewer inversions. However, as the number of repetitions increase, the projective system representation shows clear advantage in saving computational time because of the inversion operation being withheld till the last stage of computation.

b) The case for $F_k, k = 2^m$, $char(F_k) = 2$

Recalling the addition formula for j-invariant elliptic curve groups,

If $P = (x_1, y_1) \in E$ and $Q = (x_2, y_2) \in E$, then $P \oplus Q = (x_3, y_3)$ where

$$x_3 = \begin{cases} \left(\dfrac{y_2 + y_1}{x_2 + x_1}\right)^2 + x_1 + x_2, & \text{if } P \neq Q \\ \dfrac{x_1^4 + a_4^2}{a_3^2}, & \text{if } P = Q \end{cases} \tag{3.2.13}$$

and

$$y_3 = \begin{cases} \left(\dfrac{y_2 + y_1}{x_2 + x_1}\right)(x_1 + x_3) + y_1 + a_3, & \text{if } P \neq Q \\ \left(\dfrac{x_1^2 + a_4}{a_3}\right)(x_1 + x_3) + y_1 + a_3, & \text{if } P = Q \end{cases} \tag{3.2.14}$$

In projective coordinates,

$$\begin{aligned} P &= (x_1 \cdot y_1 : 1) \\ Q &= (x_2 \cdot y_2 : z_2) = \left(\frac{x_2}{z_2} : \frac{y_2}{z_2} : 1\right) \end{aligned} \tag{5.1.20}$$

To find $R = (x_3' : y_3' : 1)$,

we get by substituting Equation (5.1.13) in (3.2.13) and defining

$$\begin{aligned} A &= (z_2 y_1 + y_2) \\ B &= (z_2 x_1 + x_2) \end{aligned} \tag{5.1.21}$$

$$\begin{aligned} x_3' &= \frac{A^2}{B^2} + x_1 - \frac{x_2}{z_2} \\ y_3' &= \frac{A}{B}\left(\frac{A^2}{B^2} + \frac{x_2}{z_2}\right) + 1 + y_1 \end{aligned} \tag{5.1.22}$$

Defining $z_3 = B^3 z_2$, $x_3 = x'_3 z_3$ and $y_3 = y'_3 z_3$ to get

$$P \oplus Q = (x_3 : y_3 : z_3) \tag{5.1.23}$$

where

$$\begin{aligned} x_3 &= A^2 B z_2 + B^4 \\ y_3 &= (1 + y_1) z_3 + A^3 z_2 + A B^2 x_2 \\ z_3 &= B^3 z^2 \end{aligned} \tag{5.1.24}$$

This addition formula requires nine multiplications, two more than affine addition But this is computation overhead is offset by not having to perform costly inversion at each step

Example: Consider the computation time comparison for the elliptic curve group E . $y^2 + y = x^3 + x + 1$ over $\dfrac{F_{2^{17}}}{x^{17} + x^3 + 1}$ and point $(\alpha^{787}, \alpha^{58941})$ being repeatedly added. We observe that projective coordinate system offers clear advantage over the affine coordinate system for large values of repetitions (similar to the previous example).

5.2 Choice of Basis representation

In our entire analysis (encryption and decryption), the basic problem involves the following: given a point $P \in E(F_k)$ over a field F_k, find a point $Q \in E(F_k)$ such that $Q = \eta P$, where $0 < \eta \leq \#E(F_k)$.

So a proper choice of basis function becomes very important to reduce the computational time involved in elliptic curve algebra. We start with the Standard Basis representation.

5.2.1 Standard Basis Representation

Consider any field F_{q^m} of characteristic q generated by an irreducible polynomial $f(x)$ with α being the primitive element ($f(\alpha) = 0$). Then any element of $A(\alpha) \in F_{q^m}$ can be represented as

$$A(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdot\ \cdot + a_{m-1}\alpha^{m-1} \tag{5.2.1}$$

such that $a_i \in \{0, 1, \cdots, q-1\} \qquad \forall i \in \{0, 1, \cdots, m-1\}$

This is known as the Cartesian or Standard Basis representation of any element in F_{q^m}. In this representation, the addition operation is easy to compute. If $A(\alpha) + B(\alpha) = C(\alpha)$, then addition occurs as

$$a_i + b_i = c_i \qquad \forall i \in \{0, 1, \cdots, m-1\} \tag{5.2.2}$$

Whereas the product $A(\alpha).B(\alpha)$ is more difficult to compute. More particularly, consider $A^2(\alpha)$ where $A(\alpha) \in F_{2^m}$.

$$\begin{aligned} A^2(\alpha) &= (a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1})^2 \\ &= a_0^2 + a_1^2\alpha^2 + \cdots + a_{m-1}^2\alpha^{2(m-1)} \\ &= a_0 + a_1\alpha^2 + \cdots + a_{m-1}\alpha^{2(m-1)} \end{aligned} \tag{5.2.3}$$

which is not in standard basis notation, since the terms corresponding to $(\alpha, \alpha^3, \cdots)$ are not present and thus the result is not in the form of

$$C(\alpha) = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{m-1}\alpha^{m-1} \tag{5.2.4}$$

To overcome this difficulty in multiplication, we use a Normal Basis representation.

5.2.2 Normal Basis representation

Consider an element $\beta \in F_{q^m}$ such that $\{\beta, \beta^q, \cdots, \beta^{q^{m-1}}\}$ forms a linearly independent set. Then any element $A(\beta) \in F_{q^m}$ can be represented in Normal Basis notation as

$$A(\beta) = a_0\beta + a_1\beta^q + \cdots + a_{m-1}\beta^{q^{m-1}} \tag{5.2.5}$$

and

$$A^q(\beta) = a_0^q\beta^q + a_1^q\beta^{q^2} + \cdots + a_{m-1}^q\beta^{q^m} \tag{5.2.6}$$

and since $\beta^{q^m} = \beta$ over F_{q^m}, we have,

$$A^q(\beta) = a_{m-1}\beta + a_0\beta^q + \cdots + a_{m-2}^q\beta^{q^{m-1}} \tag{5.2.7}$$

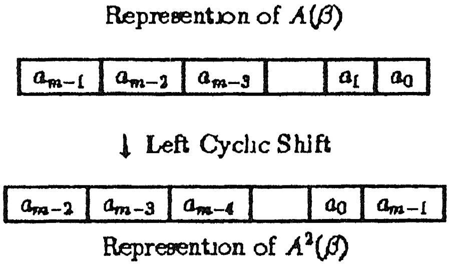
Table 8: Polar to Cartesian Coordinate Mapping

Polar	Cartesian		
	α^2	α †	1
0	0	0	0
1	0	0	1
α	0	1	0
α^2	1	0	0
α^3	1	0	1
α^4	1	1	1
α^5	0	1	1
α^6	1	1	0

Table 9: Normal Basis Representation

Elements	Normal Basis Form		
	α^4	α^2	α †
0	0	0	0
1	1	1	1
α	0	0	1
α^2	0	0	1
α^3	1	0	1
α^4	1	0	0
α^5	1	1	0
α^6	0	1	1

Figure 7: Squaring Operation of any element $A(\beta$ ‡$) \in F_{2^m}$



† *α is a primitive root of the irreducible polynomial $f(x) = x^3 + x^2 + 1$ which generated F_{2^3} i.e $f(\alpha) = 0$*

‡ *The conjugacy class containing β forms a basis representation of the elements of F_{2^m}*

Considering $q = 2$, this has a simple interpretation as shown in Figure 7. Given an element $A(\beta)$ stored in a register, a squaring operation is one left cyclic shift, quadrupling operation is two left cyclic shifts and so on.

Every field F_{q^m} has at least one element β such that $\{\beta, \beta^q, \cdots, \beta^{q^{m-1}}\}$ is a linearly independent set.

Example: Consider F_2^3 generated by the irreducible polynomial $f(x) = x^3 + x^2 + 1$ and let α be a primitive element.

Consider the set $\{\alpha, \alpha^2, \alpha^4\}$.

The mapping from polar to cartesian representation for the above field is shown in Table 8.

Rank of the matrix

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

is 3. Hence it can be chosen as a basis set for normal basis representation. Accordingly the elements of this field can be represented in the new basis system as shown in Table 9.

Considering the group operation for elliptic curve cryptosystems, where most of the computation time is taken up by multiplication operation, we shall use normal basis representation while carrying out computations for encryption and decryption schemes.

However, this is not necessarily the optimum † choice of basis functions. However, for a lack of a better basis set for easier computation, we shall use normal basis representation in our work.

5.3 Some Efficient Encryption Schemes

Consider an elliptic curve group $E(F_k)$ defined over a field F_k. The standard procedure to compute the ciphertext $c = \eta P$ where message text $m = P$, a point defined on the elliptic curve and $\eta \in Z$, is to calculate it as

$$\eta P = (\cdots(((P \oplus P) \oplus P) \oplus P) \oplus \cdots P) \qquad (5.3.1)$$

† *optimum in the sense of minimising the computation time for group operations*

Computation Time Comparison for Standard and Efficient Methods of Group Operation

Table 10.a: $E\ \ y^2 = x^3 + x + 1$ **over** F_{234161}, **point** (73292, 887013)

Repetitions	Standard Method (in sec)	Efficient Method (in sec)
771	0 049280	0 005360
5857	0 375424	0 010256
11538	0 789512	0 011384
38101	2.438464	0 013632
97652	6 689012	0 017064
158321	10 529920	0 020316

Table 10.b: $E\ \ y^2 + y = x^3 + x + 1$ **over** $\frac{F_{2^{23}}}{x^{23} + x^5 + 1}$, **point** $(\alpha^{45311}$ †, $\alpha^{70851})$

Repetitions	Standard Method (in sec)	Efficient Method (in sec)
7533	0 482112	0 007468
25519	1 833216	0 009320
61777	4.053720	0 018824
97351	7 230400	0 017976
376609	24 102976	0 022312
931672	64 711004	0 066256

† *α is a primitive root of the irreducible polynomial* $f(x) = x^{23} + x^5 + 1$ *which generates* $F_{2^{23}}$ *i.e* $f(\alpha) = 0$

But this procedure involves $(\eta - 1)$ steps to calculate the cipher. A second and a more efficient method [1] is realised as

$$\eta P = k_{\eta_0} P \oplus k_{\eta_1} 2P \oplus k_{\eta_2} 4P \oplus \cdots k_{\eta_{n-1}} 2^{n-1} P \tag{5.3.2}$$

where $k_{\eta_i} \in \{0,1\} \quad \forall \in \{0,1,\cdots,n-1\}$.

This method is a very useful because it can be easily implemented using systolic array processors.

Example:

$$\begin{aligned} 15P &= P \oplus 2P \oplus 4P \oplus 8P \\ &= (((P \oplus 2P) \oplus 4P) \oplus 8P) \end{aligned}$$

It is found that the number of operations n (one operation is adding two points on $E(F_k)$) is bound as

$$m + 1 \le n \le 2m + 1 \tag{5.3.3}$$

where $m = \lfloor log_2 \eta \rfloor$ The expected number of operations for all values of η of length n is $1.5m + 1$.

Example: Consider the elliptic curve group $E : y^2 = x^3 + x + 1$ over F_{234161} and a point $(73292, 887013)$ which belongs to the group Simulation was done in C language to compare times for the standard and efficient methods of implementing group operation (See Table 10.a) It is found that the improvement in time taken is spectacular for large values of repetitions (order of 10^3 or more). This is because the time taken increases approximately linearly for the standard technique whereas for the efficient method, it increases only in a logarithmic fashion. A similar exercise was carried out for the case of $E : y^2 + y = x^3 + x + 1$ over $\frac{F_{2^{23}}}{x^{23} + x^5 + 1}$, point $(\alpha^{45311}, \alpha^{70651})$, (See Table 10 b) and similar results were obtained.

Chapter 6
Conclusions

We conclude our discussion with a comparison with existing cryptosystems and discuss the scope for further work in this area.

6.1 Comparison with existing Public-Key Cryptosystems

In our analysis, we have presented elliptic curve analogs of the existing public-key cryptosystems and have discussed the computational issues involved with them. In this section, we shall first compare the computational timings for encryption using the traditional RSA scheme for public-key systems and the proposed Generalised Elliptic Curve scheme which is the equivalent of RSA scheme based on elliptic curve algebra.

6.1.1 Computation Time Comparison

For this, we choose operations over the ring Z_n where n is a product of two primes $p_1 = 9857$ and $p_2 = 9839$ and $n = 96983023$. For the RSA case, consider a message $m_{rsa} = 13331$ to be encrypted and the public-key available as $e_{rsa} = 53293$. The message m_{rsa} can be represented as a two-tuple vector $(m^1_{rsa}, m^2_{rsa}) = (3474, 3492)$ where $m^1_{rsa} \in Z_{9857}$ and $m^2_{rsa} \in Z_{9839}$, similarly the public-key e_{rsa} can be represented in a two-tuple form as $(\mathrm{e}^1_{rsa}, \mathrm{e}^2_{rsa}) = (4008, 4098)$ where $\mathrm{e}^1_{rsa} \in Z_{9857}$ and $\mathrm{e}^2_{rsa} \in Z_{9839}$ The operation of encryption given by $c_{rsa} = m^{e_{rsa}}_{rsa}$ can be equivalently viewed as computing $\underline{c_{rsa}} = (c^1_{rsa}, c^2_{rsa}) = \left((m^1_{rsa})^{e^1_{rsa}}, (m^2_{rsa})^{e^2_{rsa}}\right) = \left((3474)^{4008}, (3492)^{4098}\right)$ where $c^1_{rsa} \in Z_{9857}$ and $c^2_{rsa} \in Z_{9839}$. Finally, on computing the two-tuple pair (c^1_{rsa}, c^2_{rsa}), we compute $c_{rsa} \in Z_{96983023}$ using CRT Notice that the two operations can be carried out in parallel and later combined using CRT We simulated the above process using C language source code and observed that the process output which is the ciphertext c_{rsa} was $c_{rsa} \equiv 24237098 \pmod{\phi(n)}$ where $\phi(n) = (p_1 - 1)(p_2 - 1) = 96963328$ and the time taken for computation was around 0.012976 sec (operating at a clock rate of 15625 ticks per second).

Similarly, consider the elliptic curve $E : y^2 = x^3 + 1$ defined over $Z_{96983023}$ Now, both $p_1 \equiv 2 \pmod 3$ and $p_2 \equiv 2 \pmod 3$ and hence the order of the two abelian (cyclic) groups $E(Z_{p_1})$ and $E(Z_{p_2})$ is given by $\#E(Z_{p_1}) = 9858$ and $\#E(Z_{p_2}) = 9840$ respectively. Consider a message point given by $m_{gec} = (14321, 5859531) \in E(Z_n)$ and the public-key available be $e_{gec} = 53293$ (same as the case above). The message m_{rsa} can be represented as a two-tuple vector $(m^1_{gec}, m^2_{gec}) = \big((4464, 3909), (4482, 5326)\big)$ where $m^1_{gec} \in E(Z_{9857})$ and $m^2_{gec} \in E(Z_{9839})$, similarly the public-key e_{gec} can be represented in a two-tuple form as $(e^1_{gec}, e^2_{gec}) = (4008, 4098)$ where $e^1_{gec} \in Z_{9857}$ and $e^2_{gec} \in Z_{9839}$. The operation of encryption given by $c_{gec} = e_{gec}.m_{gec}$ can be equivalently viewed as computing $\underline{c_{gec}} = (c^1_{gec}, c^2_{gec}) = (e^1_{gec}.m^1_{gec}, e^2_{gec}.m^2_{gec}) = \big(4008(4464, 3909), 4098(4482, 5326)\big)$ where $c^1_{gec} \in E(Z_{9857})$ and $c^2_{gec} \in E(Z_{9839})$. Finally, on computing the two-tuple pair (c^1_{gec}, c^2_{gec}), we compute $c_{gec} \in E(Z_{96983023})$ using CRT. On simulation, the ciphertext was found to be $c_{gec} \equiv (7439209, 90875269) \pmod{\#m}$ where $\#m = lcm\big(\#E(Z_{p_1}), \#E(Z_{p_2})\big) = lcm(9858, 9840) = 5389040$ and the time taken for computation was around 0.078636 sec

Hence, in a direct comparison of timings of the RSA scheme and the Generalized Elliptic Curve scheme † , we find that RSA method is computationally superior *i.e* it is around six times as fast as the analogous elliptic curve system. However, it is only natural to expect this as the amount of computation required for elliptic curve system is far more complex than the RSA scheme where only a modulo multiplication is required at each step. Hence it can be safely conjuctured that the major slowing down factor for elliptic curve systems vis-a-vis existing public-key cryptosystems lie in the computational complexity involved in the group operation.

Also one critical fact is that there is a message bandwidth expansion while using an elliptic curve cryptosystem as now we have to transmit two coordinates (x, y) instead of one, as in traditional cryptosystems. However, by a proper choice of the elliptic group (like the classes over F_{2^m}, m odd) we need to transmit only information of the trace function of y for a given x, which is only one bit long, either 0 or 1 since ground field is F_2. Thus the message bandwidth expansion is almost negligible for these special cases.

However, this penalty that we pay is for the benefit of greater amount of security that elliptic curve cryptosystems offer.

† *here the order of the group, message texts and encryption keys have been taken as similar as possible in the two cases to facilitate a meaningful comparison*

6.1.2 Comparison on Security Aspects

In Chapter 1, we had expressed the hope that working on a more general framework of groups and monoids, we would be able to ward off many of the cryptanalytic attacks that occur on a more restricted framework of fields and rings. Using the example of elliptic curve cryptosystems, we shall see that it is indeed so.

Using cryptosystems based on the field structure, like Pohlig-Hellman, El Gamal, etc., we have to keep the hide the order of the multiplicative group over which our cryptosystem is based else all the ciphertexts are very easily decrypted by cryptanalysis. Also the multiplicative group structure is the focal point of evaluating discrete logarithm method of attacks (like Index Calculus methods, etc). Hence, for a safe cryptosystem, one is left with the option of working in very high orders of groups which guarantee security.

In cryptosystems based on ring structure Z_n, like RSA scheme, where n is a product of very large primes, we can let out the parameter n.The security of the system is based on the difficulty of factoring a large number which is considered one of the most intractable problems in number theory. However, in recent past [4], there have been major improvements in solving factorization problems (reported upto 100 decimal digits). Hence, cryptosystems based on smaller factors are now being seriously threatened.

Considering all this, attempts have been made to base the cryptosystems on a more general structure, notably the elliptic curve groups and matrix ring groups [22]. Since all that we need is structure over which we can define a permutation operator, group structures amply satisfy this requirement. Also, since the group operation is addition (denoted by $\oplus$), the discrete logarithm attacks based on present methods become inoperative. One of the major advantages of using elliptic curve groups is that we can have added security by changing the curve periodically Moreover, in order to break the cipher one would need an algorithm for solving the discrete logarithm problem over an arbitrary elliptic curve, rather than just on a particular elliptic curve. The major saving on changing periodically is that we can base the cryptosystem on much smaller orders of groups *i.e* we can continue using existing cryptosystems with suitable modifications.

In the further generalization that we have made *i e* basing cryptosystems over monoid, we have added advantages over the RSA scheme The security of the system is two-fold one, the integer factorization problem, and two, the fact that we hide the elliptic curve makes it almost impossible for a cryptanalyst to estimate the order of the abelian groups. Here again, we have the advantage of working in much smaller orders of n and thus smaller key lengths, which can be crucial in some applications, for example the design of smart card systems.

6.2 Scope for Future Work

Since the present work is essentially a study at a conceptual level and substantiating upon it with simulation results, some of the aspects which arise on practical implementation like confusion, diffusion, etc. which are important because of high redundancy of the source language have been necessarily excluded from the analysis. A detailed study of these aspects is required for a more complete picture of the problem.

Currently, attempts are being made to build a dedicated RSA chip based on VLSI design In a similar way, we can try to fabricate a dedicated elliptic curve cryptosystem chip with suitable modifications to the RSA chip design.

Complexity analysis of the various algorithms used for elliptic curve encryption and decryption can be carried out so that we can base our design decisions on what we believe to be the best algorithms.

One of the major problems for the slow bit rate of these systems is the complicated group algebra involved A detailed study needs to be carried out to search for a proper choice of basis function for making these operations more efficient.

We could also view from a much more abstract level *i.e* considering the entire problem as one of a proper choice of an operator † over finite fields and rings with desired properties vis-a-vis security aspects and computational complexity. Maybe, we could find specific instances of operators with lesser computational complexities (which translate to faster encryption and decryption rates) but guaranteeing same levels of security *i.e* time estimates for cryptanalytic attacks are similar

† *elliptic curve operator or matrix ring operators being only specific cases*

References

[1] Agnew, G.B, Mullin, R.C. and Vanstone, S.A. "A Fast Elliptic Curve Cryptosystem", Advances in Cryptology - Eurocrypt '89, Springer-Verlag (1989), 705-707.

[2] Blake, I, Menezes A.J. *Applications of Finite Fields*, Boston, Klewer Academic Publishers, 1993.

[3] Bender, A. and Guy Castagloni "On the implementation of Elliptic Curve Cryptosystems", Advances in Cryptology - Crypto '89, Springer-Verlag (1990), 186-192.

[4] Bach, Eric "Intractable problems in Number Theory", Advances in Cryptology - Crypto '88, Springer-Verlag (1988), 77-93.

[5] Brassard, Gilles "Modern Cryptology" - A Tutorial, Springer-Verlag (1988).

[6] Chachal, J.S. *Topics in Number Theory*, Plenum Press, New York 1988.

[7] Chin Long Chen "Formulas for solving quadratic equations over $GF(2^m)$", IEEE Trans. Info. Th, 28 (1982), 792-794.

[8] Chum, David and Jorge, W.de "Some variations of RSA signatures and their security", Advances in Cryptology - Crypto '86, Springer-Verlag (1986), 49-59.

[9] Coppersmith, D. "Fast Evaluation of logarithm in fields of characteristic two", IEEE Trans. Info. Th, 30 (1984), 587-594.

[10] Denning, Dorothy E. *Cryptography and Data Security*, Addison-Wesley, 1982.

[11] El Gamal, T. "A subexponential-time algorithm for computing discrete logarithm over $GF(p^2)$", IEEE Trans. Info. Th, 31 (1985), 473-481.

[12] Kaliski Jr. B.S. "A Pseudo-Random Bit Generator based on Elliptic logarithms" Advances in Cryptology - Crypto '86, Springer-Verlag (1986), 84-103.

[13] Koblitz, N. "Constructing Elliptic Curve Cryptosystems in Characteristic 2", Advances in Cryptology - Crypto '90, Springer-Verlag (1991), 705-707.

[14] Koblitz, N. "Elliptic Curve Cryptosystems", Mathematics of Computation, 48 (1987), 203-209.

[15] Lidl, Rudolf and Niederreiter, Harald *Introduction to finite fields and their applications*, Cambridge Univ. Press 1986.

[16] Menezes, A. and Vanstone, S.A. "The implementation of Elliptic Curve Cryptosystems", Advances in Cryptology - Auscrypt '90, Springer-Verlag (1990), 2-13.

[17] Miller, V. "Use of Elliptic Curves in Cryptography", Advances in Cryptology - Crypto '85, Springer-Verlag (1986), 417-426.

[18] Niven, Ivan and Zuckerman, H.S. *An Introduction to the Theory of Numbers*, Wiley-Eastern, Third Ed. 1976.

[19] Pohlig and Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance", IEEE Trans. Info. Th, 24(1978), 106-110.

[20] Schoof, R.J. "Elliptic Curve over finite fields and the computation of square roots mod p", Mathematics of Computation, 44 (1985) 483-494.

[21] Stephens, N.M. "Lenstra's Factorization Method based on Elliptic Curves", Advances in Cryptology - Crypto '85, Springer-Verlag (1985), 409-416.

[22] Varadarajan, V. "Trapdoor Rings and their use in Cryptography", Advances in Cryptology - Crypto '85, Springer-Verlag (1985), 369-395.

Errata

1 Page 9, Definition, read $\phi(n)$ *is the number of positive integers less than or equal to* n instead of $\phi(n)$ *is the number of positive integers less than to* n

2. Page 10, Equation (2.4.4), read $a^{\phi(n)} \equiv 1 \ mod n$ instead of $a^{\phi(n)} \equiv 1 \ mod p$.

3 Page 10, Equation (2 4 5) read $m \in Z_p$ instead of $m \in Z_n$, $c \in Z_p$ instead of $C \in Z_p$.

4 Page 11, Equation (2.4 8), read "$e = log_m c \cdots$" instead of "$c = log_m c \cdot \ \cdot$".

5. Page 58, line 8, read "$m' = (58,14) \oplus (11,59) \cdots$" instead of "$m' = (58,14) \oplus (58,65) \ \cdot\cdot$"

6. Page 61, Equation (5 1.11), read " $\ \cdot = X^3 + a_2X^2Z + \ \cdot$ " instead of " $\cdot\cdot = x^3 + a_2X^2Z + \cdots$"

7. Page 68, Equation (5.2.7), read "$A^q(\beta) = \cdots + a_{m-2}\beta^{q^{m-1}}$" instead of "$A^q(\beta) = \cdots + a^q_{m-2}\beta^{q^{m-1}}$".